VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra Elektroenergetika

Moderní systémy řízení provozu budov vč. sledování pohybu osob.

Modern wiring system including personal monitoring in public bulding.

2011 *Bc. Miroslav Milata*

Prohlášení

„Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Datum odevzdání diplomové práce:

Podpis:

Abstrakt

Mezi hlavní záměry této diplomové práce je představit nejnovější technologie v automatizaci budov, zejména zaměřené na integraci jednotlivých systémů. Ve druhé části je práce zaměřena na systémy bezpečnostní, jejich vzájemnou integraci a na návrhu systému kontroly přístupu a oprávnění v administrativní budově, kontroly vstupu a perimetrickou ochranu areálu. Součástí návrhu je v poslední části zpracován ekonomický rozbor investice.

Between the main intentions of this thesis is to introduce the latest technology in automation of buildings, in particular aimed at the integration of individual systems. In the second part of the work is focused on systems security, their mutual integration and on the design of the system of access control and permissions on the administrative building, access control and perimetrickou protection area. Part of the proposal is processed in the last part of the economic analysis of investments.

Klíčová slova

Automatizace budov; integrace systémů; kontrola přístupu; perimetrická ochrana; sběrnice; management energií; protokol; biometrické systémy; čtecí modul; systémová technika budov; technická zařízení budov; smart karta; identifikace RFID.

Building automation; integration systems; access control; perimeter protection; energy management; bus; Protocol; biometric systems; reader module; system building technology; technical equipment of buildings; smart card; RFID identification.

Obsah

1. Úvod

Tato diplomová práce zpracovává analýzu a návrh začlenění automatizovaného systému budov do praxe v areálu a objektu administrativního střediska.

V první části představuji základy komunikačních systémů, jejich typy a vzájemnou integraci v automatizaci budov. Dále základní softwarové a hardwarové komponenty a zařízení v obecné rovině. Další kapitola se zabývá vlastním návrhem a kalkulací integrovaných systémů v kancelářské budově včetně přilehlých prostranství Správního střediska.

2. Úvod do automatizace budov

2.1. Význam automatizace budov

Již řadu let roste podíl automatizace, jak v soukromé a rodinné bytové výstavbě, tak i v účelových stavbách. Pod pojmem „účelové stavby" rozumíme budovy, které plní určité funkční zaměření. Patří sem například kancelářské budovy, nákupní střediska nebo hotely. Tento druh staveb se svým přesně vymezeným zaměřením odlišuje od obytných budov.

Tento růst má svou příčinu jednak v rostoucích nárocích uživatelů na komfort, ale také ve velkém významu automatizace budov pro úsporu energie a řízení její spotřeby. V bytové výstavbě k tomu ještě přistupuje aspekt zajištění bezpečnosti, kdežto v účelových stavbách se vyžaduje vysoká flexibilita tak, aby bylo v budoucnu možné změnit účel a využití budovy. [1].

2.2. Automatizace budov v soukromé bytové výstavbě

V současné době u soukromé bytové výstavby vidíme, že se značný počet automatizovaných funkcí stává určitým standardem. Za samozřejmost je považována regulace spotřeby energie, kdy optimalizované regulační funkce jsou integrovány do systému vytápění. Do komponent regulace teploty výrobci běžně integrují programy na časování a sepnutí režimu snížené noční spotřeby. Tyto programy se postupně staly samozřejmostí a u většiny nových instalací fungují v plném rozsahu již od okamžiku uvedení do provozu. Hlavním aspektem je zde energetická úspornost. Jako další příklad automatizace funkcí v soukromé bytové výstavbě můžeme uvést řízení osvětlení. V mnoha případech se vnější osvětlení obytných domů samočinně spíná instalovaným senzorem pohybu. I když jde jen o poměrně jednoduchou automatizační funkci, její řešení představuje již spojení řízení události s logickou operací. Zde je na prvním místě aspekt pohodlí.

Daleko komplikovanější situace nastane, jestliže se má osvětlení celého obytného domu zapínat a vypínat z jednoho místa. Pokud by se toto zadání mělo řešit pouze konvenční

elektroinstalací, pak by se to dalo uspokojivě provést jen se značně rozsáhlými kabelovými rozvody. Zcela nové možnosti se však objeví, když se použijí sběrnicové systémy a s nimi související komunikace mezi všemi komponenty, které osvětlení ovládají. Centrálním spínačem umístěným v ložnici lze spustit i alarm v případě nočního vloupání. Zde se v první řadě jedná o zajištění bezpečnosti.

V souhrnu lze uvést, že automatizované funkce v soukromé bytové výstavbě získaly velký význam zejména v oblastech:

- hospodárnosti a úspory energií,
- komfortu,
- bezpečnosti.

[1].

2.3. Automatizace budov v účelových stavbách

V dnešních účelových budovách se nachází množství různých automatizačních systémů. Například kromě zařízení na výrobu tepla jsou to hlavně instalace chladicích zařízení a vzduchotechniky. Protože se jedná o podnikatelsky provozované objekty, vybavují se zpravidla náročnými řídicími a regulačními systémy. Ty pak zajišťují bezvadný chod jednotlivých zařízení, která jsou v mnoha případech vzájemně propojeny a spojeny dispečerským řídicím stanovištěm. Komunikaci pak zajišťuje systém datových sběrnic a sítí. Vedle optimalizace spotřeby energií se

Obr. 1 Vzduchotechnické zařízení

projeví úspory i ve snižování počtu pracovníků obsluhy. Průzkumy výkonnosti zaměstnanců zjistily, že nejvyšších výkonů dosahují v příjemném prostředí a jejich výkonnost značně klesá, když jsou například v létě vystaveni vysokým teplotám. To vedlo k tomu, že se kancelářské místnosti v nových

budovách stále častěji vybavují klimatizací a ventilací. Ovládání těchto systémů v kancelářích se rovněž značně mění. Žaluzie nebo osvětlovací tělesa jsou dnes ovládána z pracovního místa osobním počítačem nebo automaticky neustálým vyhodnocováním velikosti intenzity slunečního záření. Obojí přispívá k růstu komfortu a vyšší výkonnosti pracovníků.

Další požadavek na systémy v těchto budovách vyplývá z chování uživatelů. Požadavky na rozdělení pracovního prostoru se mohou například měnit v závislosti na restrukturalizaci firmy. Místo velkých konferenčních místností můžou vznikat menší kanceláře, na což se pamatuje už u projektování stavby. Její konstrukce a dispozice budovy včetně provozně - technického vybavení musí takové změny umožnit. Například při přestavbě prostorů rozmístění světelných vypínačů a jejich přiřazení k příslušným světelným zdrojům už nevyžaduje elektrické propojení kabely, ale přizpůsobení změně se provede přeprogramováním inteligentních komponent. Vidíme, že se zde dostává do popředí aspekt flexibility pracovního prostředí.

Úhrnem lze konstatovat, že automatizace budov nabývá v účelové výstavbě na významu zejména v oblastech:

- zajištění hospodárnosti provozu a úspor energií,
- komunikace prostřednictvím sběrnicových systémů a sítí,
- komfortu,
- flexibility.

[1].

2.4. Pojmy v automatizaci budov a systémové techniky budov

Když mluvíme o automatizaci funkcí v budovách, zjišťujeme, že spolu s pojmem automatizace budov se používá rovněž pojem systémové techniky budov.

Automatizace budov je digitální, měřicí, kontrolní, regulační a řídicí technika pro technické vybavení budov.

Systémová technika budov je speciální částí automatizace budov, která se přednostně zabývá elektroinstalací a popisuje propojení sítí, sestavených ze systémových komponent a účastnických stanic pomocí instalační sběrnice (Installation Bus) do jednoho systému, spojeného s elektroinstalací, zajišťující jeho provozní fungování. Inteligence systému je rozdělována na jednotlivé komponenty, informační toky probíhají přímo mezi jednotlivými účastníky.

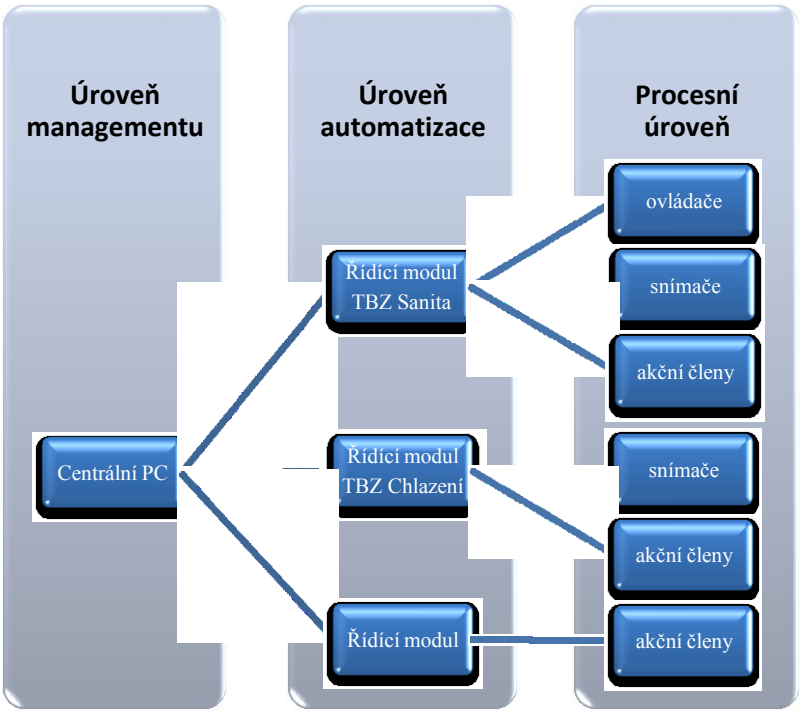
Komponenty systémové techniky budov se montují většinou přímo do podřízených elektrorozvodů, ale také se mohou montovat přímo do řízených modulů. V technice systémů budov nejsou zapotřebí žádné další centrální řídicí jednotky.

Technické zařízení budov (TZB) zahrnuje množství zařízení, která jsou pro provoz budov nezbytná. Mezi nejdůležitější technické zařízení patří taková, která zajišťují vnitřní prostředí budovy.

Můžou to být zařízení, která umožňují dodávku tepla, chladicích médií, čerstvého vzduchu, vody a elektrické energie. Dále se můžeme zmínit o zařízení na likvidaci odpadů, zařízení pro kanalizaci a odpadní vody, výtahy a zdviže atd. Klasifikace tzv. technických zařízení a vybavení budov se řídí podle odborných profesí, které tato zařízení instalují. Aby v dnešní době mohla tato zařízení automaticky a hospodárně fungovat, musí být vybavena příslušnými regulačními a řídícími moduly.

Automatizační a řídicí systémy budov přejímají v systému koordinační a integrační roli, která vyžaduje zajištění propojení, což je možno realizovat třemi způsoby:

- Za prvé se TZB může řídit a regulovat vestavěnými řídicími jednotkami a komponentami, které jsou integrovány do systémové techniky budovy. Toto je obvyklé u TZB, jakými jsou vytápění, větrání a klimatizace.
- Za druhé - integraci je možno zajistit prostřednictvím speciálních řídících modulů, které nebudou samy provádět řídicí funkce, ale zajistí monitoring, vstupní a výstupní konektivitu. To je obvyklé u TZB, která jsou vybavena vlastními automatizačními prostředky. Tento způsob se používá u TZB sanity a zajištění dodávek elektrické energie.
- Za třetí - u této varianty je zajištěna přímé spojení mezi příslušným TZB a řídicím počítačem v rámci sítě. Je vhodná zejména tam, kde se přenáší velký objem dat, anebo tam, kde má připojené TZB vlastní počítač. V tomto případě se přenos dat realizuje bez rozsáhlých kabelových rozvodů, prostřednictvím sběrnice anebo v síti. To je vhodné například u integrace podřízených (Slave) videosystémů, anebo u nadřazeného systému (Master) vyúčtování a úhrad.



Automatizační a řídicí systém budov přizpůsobuje a integruje z informačně - technického hlediska jednotlivá zařízení budov do jednoho celku a umožňuje jejich centrální monitorování a řízení počítačem na úrovni managementu (obr. 2).

Obr. 2 Integrace technických zařízení budov do systému automatizace a řízení budov

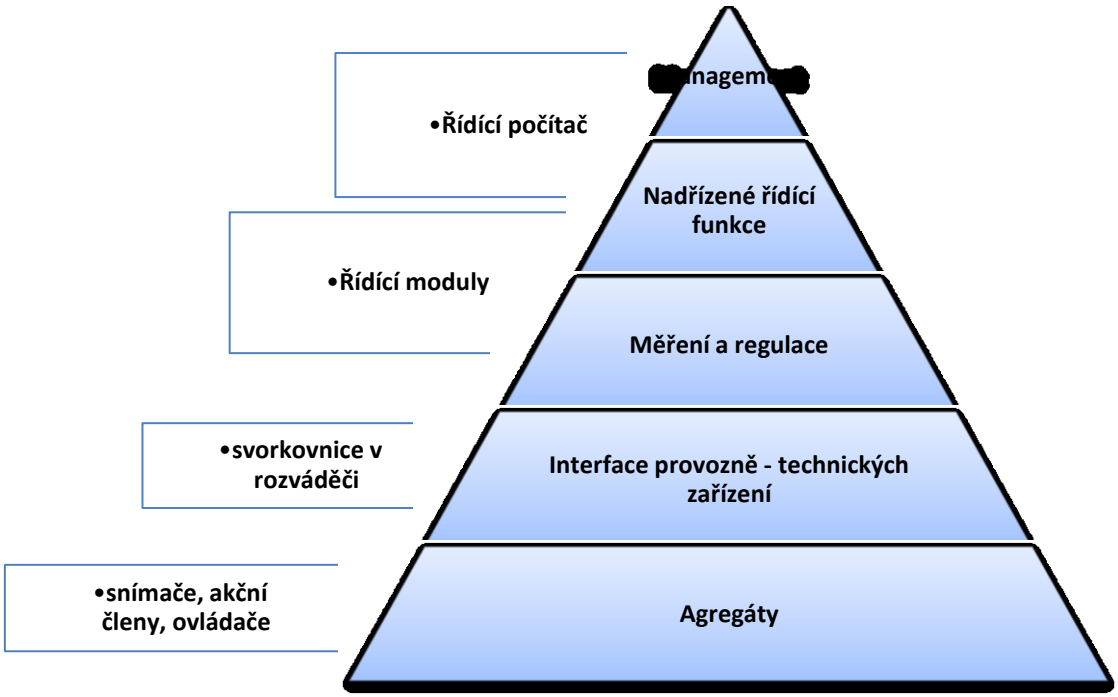
Přehled automatizace a řízení budov společně s technickým zařízením budov (TZB), jež zahrnují, je uvedena v tabulce *Tab.1* [1].

Zařízení TZB	TZB běžně integrovaná do automatizace budov	TZB dodatečně integrovaná do automatizace budov	TZB s řídícími moduly nebo s řízením a regulací prostřednictvím komponent techniky systémů budov
Vytápění	X		X
Chlazení	X		X
Ventilace	X		X
Dodávky el. energie	X		
Řízené osvětlení	X		X
Řízení žaluzií (zastínění)	X		X
Sanitární zařízení	X		
Detekce a ohlašování požáru	X		
Detekce a ohlašování neoprávněného vstupu		X	
Kontrola vstupu do budovy		X	
Domovní kamerový a video systém		X	
Technika sítě - zasíťování		X	
Multimedia		X	
Výtahy		X	
Telefonní přístroje		X	
Údržba		X	
Systém vyúčtování a úhrad		X	
Facility Management		X	

Tab. 1 TZB v automatizaci a řízení budov

2.5. Víceúrovňová struktura automatizace budov

Při popisu komponent nezbytných pro výkon monitorovacích a řídicích funkcí se uplatňuje všudypřítomná víceúrovňová struktura. Na obrázku č. 3 je zobrazena nejčastěji uváděná hierarchická struktura automatizace budov. V blízkosti procesů jsou umístěny snímače, nutné pro zachycení informací a dat o systému. V integrovaném systému automatizace budov jsou to na této nejnižší úrovni snímače teploty, průtokoměry, ale také snímače pro snímání stavu, jako jsou např. hlídače námrazy a vlhkosti. K tomu přistupují akční prvky, které umožňují vlastní řízení a ovládání provozně technických zařízení. U vzduchotechnických zařízení jsou to například ventily k regulaci průtokového množství u oběhového vytápění nebo servopohon k nastavení klapky pro zvýšení podílu venkovního vzduchu. Tyto snímače a akční členy jsou přímo namontovány do příslušného zařízení.



Obr. 3 Hierarchická struktura automatizace budov

Spojení s řídícími moduly, které podmiňuje řízení a regulaci, se zajišťuje propojením vodičů. Taktéž hlášení o stavu anebo přenos signálů snímače. Řídící moduly se instalují zpravidla do skříně rozvaděče, umístěné v blízkosti provozně - technických zařízení. Tímto umístěním se snižuje délka rozvodů a kabelových vedení. Ve skříni rozvaděče jsou umístěny svorkovnice pro připojení rozvodů. Tyto svorkovnice vytvářejí spojení s provozně - technickým přístrojem a označují se jako provozně - technický interface.

Řídící a regulační funkce se zpracovávají autonomně. Spojení s nadřazeným počítačem není v zásadě nutné. Již na této úrovni jsou v softwaru řídicích modulů obsaženy funkce, které zajišťují energeticky úsporný provoz. Tak například u vzduchotechniky se klapky přívodu vnějšího vzduchu nastavují do optimální polohy v závislosti na vnější teplotě a podle požadavku na větrání místnosti. Funkce tohoto druhu jsou však omezeny jen na jedno technické zařízení.

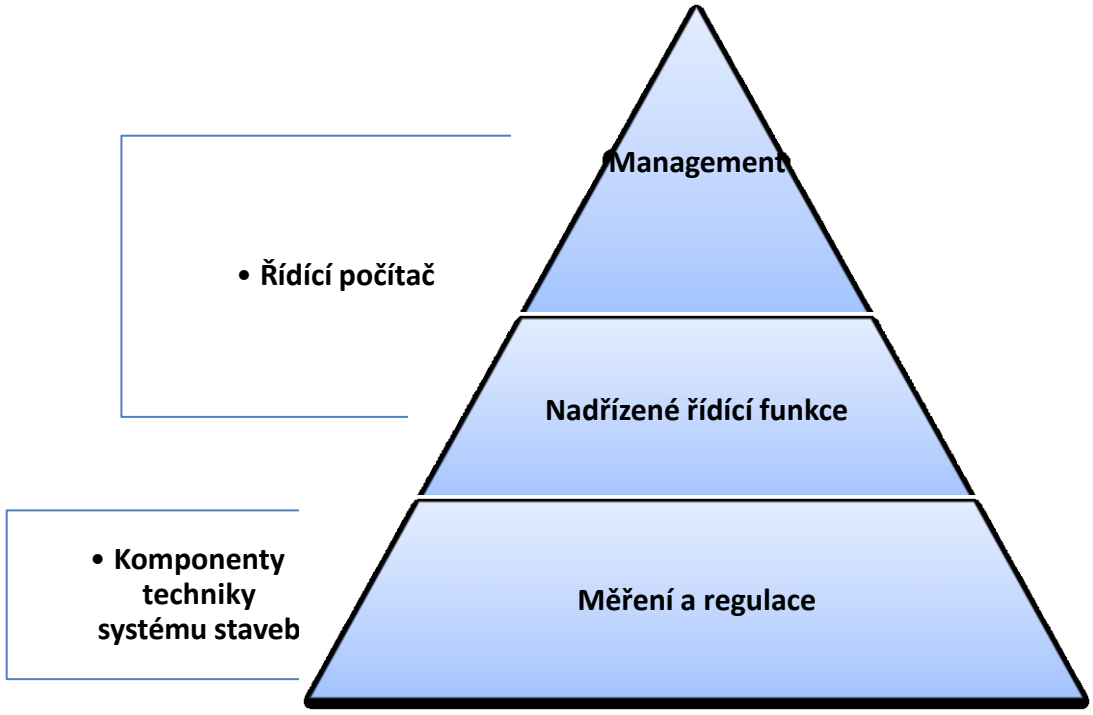
Protože u tohoto řešení se informace od všech připojených zařízení sbíhají do počítače, může převzít i jiné funkce, které nemusí patřit do automatizace technických zařízení budov. Typickým příkladem je časovací program, který je přizpůsoben provozním dobám budovy a zajišťuje ráno spuštění a odpoledne nebo večer vypnutí příslušných zařízení.

Kromě takto účelově zaměřených činností poskytuje počítač programy k řízení budovy. Na počítači jsou nainstalovány programy zajišťující funkce záznamu událostí a alarmů, archivaci naměřených hodnot a grafickou prezentaci - vizualizaci stavu provozně - technických zařízení.

Na tomto principu je pak založen přenos informací k dalším výpočetním systémům. Tak se například mohou přenášet hodnoty odečtené spotřeby energie z elektroměrů od jednotlivých spotřebitelů do systému zúčtování. [1].

2.6. Víceúrovňová struktura systémové techniky budov

Jak je vidět ze schématu na obrázku č. 4, použití komponent systémové techniky budov vytváří zcela zvláštní situaci. Kombinací vlastních snímačů, zabudovaných v jednom prostoru společně s integrovanými procesory a připojením na sběrnici, se víceúrovňová struktura redukuje v podstatě na jedinou vrstvu.



Obr. 4 Zvláštní hierarchická struktura techniky systémů

Na obrázku 4 není vidět část interface, která je uvedena na obrázku 3. Tuto funkci, včetně řídicích a regulačních funkcí, zastává vestavěný mikropočítač. Například regulace teploty probíhá okamžitě podle nastavené požadované hodnoty a výstupní signál regulátoru se po sběrnici vyšle k servopohonu ventilu, namontovanému na topném tělese.

Také obrázek 5 ukazuje systémové komponenty jednoho typu kombinace, sestávající z pětinásobného snímače s tlačítkovým ovládáním a integrovaným termostatem. Snímač se nachází přímo v přístroji a naměřenou hodnotu teploty předává k bezprostřednímu zpracování v procesoru, umístěném v tomtéž prostoru. Dodatečně je možno požadovanou hodnotu teploty místnosti nastavit a upravit programem. Pětinásobným snímačem s tlačítkovým ovládáním lze vyslat řídicí povely k akčním členům, ovládajícím lokální operace-osvětlení, stmívání, spuštění žaluzií, větrání. Horní tři

tlačítka se mohou použít k ovládání osvětlení a žaluzií. Spodní dvě tlačítka mohou sloužit k řízení světelných scén. Na druhé úrovni je možno ovládat vytápění a chlazení - na integrovaném displeji jsou pak vidět následující informace: aktuální teplota, nastavená hodnota a provozní režim. [1].

Obr. 5 Pětinásobný snímač s tlačítkovým ovládáním Busch-tríton*.

2.7. Funkce managementu energií

Jednou z nejdůležitějších úloh automatizace budov je kromě jejich automatické regulace, řízení a kontroly, zejména energeticky úsporný provoz (tzv. management energií - Energy Management).

Dnes je samozřejmé, že při projektování účelových staveb, jako jsou kancelářské budovy, nemocnice nebo nákupní centra, se bude počítat s využitím výkonné a úsporné automatizace. Důvodem je mimo jiné úspora provozních nákladů, přičemž se zvažuje, jaké úspory provozních nákladů přinese využití inteligentních řídicích funkcí.

Veškeré náklady, vzniklé v průběhu výstavby, se označují jako celkové investiční náklady výstavby. Náklady na automatizační techniku, využívanou pro automatickou regulaci a kontrolu přístroje vytápění, klimatizace a vzduchotechniky činí dle renomovaných firem 1,0 až 1,5 % celkových investičních nákladů.

Programy k optimalizaci spotřeby energií bývají velmi často zabudovány přímo do jednotlivých zařízení. Zejména je to v těch případech, kdy je není třeba pravidelně nastavovat a seřizovat a požadované funkce budou naprogramovány přímo do vestavěných řídících modulů. Tyto „napevno“ vestavěné programy mohou pracovat bez zásahů až do doby, kdy si stavební úpravy vyžádají zásadní změnu. Příkladem může být například ekvitermní regulace teploty přívodu topného okruhu, kdy snímač, který snímá venkovní teplotu podle požadované referenční hodnoty, je použit

jako regulátor vytápění. Na vysvětlenou, ekvitermní regulátor je zařízení, které reguluje topný systém na základě venkovní teploty. Tyto regulátory nabízejí více možností, více přesnosti a větší hospodárnost než prostorové regulátory. Přes kontrolu vnějšího (venkovního) a vnitřního (náběhového) čidla je regulátorem nastavována teplota vody v topném okruhu. Stejně lze takto ovlivňovat u klimatizace všechny stavy vzduchu v místnosti.

Jako další aplikací lze uvést spínání na základě řízení závislých událostí, kdy to zpočátku byly zejména instalace hlášení příchodu nebo přítomnosti osob tak, aby pokyn k řízení osvětlení se mohl vydat jen za předpokladu, že se uživatelé nacházejí v místnosti. Se složitější aplikací se můžeme setkat u zapojení jednotlivých pokojů v hotelu, kde se využívá systému rezervací od pultu recepce. V případě, že v dotyčný den nebude objednána rezervace pokoje, budou všechny spotřebiče vypnuty a referenční teplota v místnosti bude nastavena jen na přípustné minimum. Pokud se na příslušný den rezervuje místnost, bude tomu přizpůsobeno nastavení teplot. Individuální zapojení a vyregulování se může provést při vstupu návštěvníka do místnosti na základě čipové karty „Key Card".

Typicky jednoduchou funkcí managementu energie pro letní měsíce je noční chladící provoz. Smyslem je, aby se při ranním připojení funkce chlazení budovy nastavilo i značné časové zpoždění. K tomu se v průběhu nočních hodin, kdy venkovní teplota klesne pod teplotu místnosti, spínají všechna větrací zařízení a pracují s plným podílem venkovního vzduchu. Tento provoz se udržuje až do časných ranních hodin a hmota budovy a prostory jejích místností se v tomto režimu využívají jako zásobník chladicího média. [1].

2.8. Funkce řízení prostředí a managementu energií v automatizaci místností

Automatizace místností nabývá na významu jak v soukromé bytové výstavbě, tak i u účelových staveb. Zde jsou v popředí zájmu vedle komfortního prostředí a energeticky úsporného provozu zejména požadavky na vyšší flexibilitu při eventuálních budoucích přestavbách a změnách charakteru využití místností. Jestliže se například ze současné zasedací místnosti mají stát kanceláře pro nové zaměstnance, pak je možné řadu funkcí přizpůsobit novému účelu, pokud s tím bude projekt aplikace systémové techniky správně počítat. Když se v minulosti u klasické elektroinstalace měnil účel a prováděla se rekonstrukce, bylo nutné při změnách provádět rozsáhlé změny v elektroinstalaci, zapojení i v kabelových rozvodech. Dnes se takováto adaptace na nové okolnosti provede přeprogramováním instalovaných komponent systému.

Protože v bytové výstavbě se nepočítá s tak častou rekonstrukcí nebo změnou účelu místností, místo požadavku na flexibilitu nabývá většího významu aspekt zajištění bezpečnosti.

V následujícím přehledu jsou uvedeny některé funkce tvorby prostředí, a to podle jednotlivých druhů technického zařízení a vybavenosti.

Vytápění, chlazení, větrání:

- nastavení požadovaných jmenovitých hodnot pokojové teploty v závislosti na přítomnosti a počtu osob monitorováním přítomnosti nebo snímačem přítomnosti,
- vyladění hodnot pokojových teplot v hotelových místnostech, podle jejich použití a ve vazbě se systémem rezervací,
- individuální nastavení požadované pokojové teploty ovladačem,
- automatické zvýšení požadované pokojové teploty při vysokých venkovních teplotách v létě,
- vypínání funkcí vytápění a chlazení, když se otevřou okna,
- vyladění větrání v závislosti na kvalitě vzduchu v místnosti.

Řízení osvětlení:

- spuštění osvětlení ovladačem nebo snímačem přítomnosti osob,
- nastavení osvětlení v hotelových pokojích podle použití a ve vazbě na systém rezervací,
- ovládání konstantního osvětlení snímačem jasu v místnosti,
- regulace osvětlení podle jasu venkovního prostředí,
- regulace rozptýleného světla nastavením lamel žaluzií podle intenzity slunečního svitu,
- osvětlení vnější fasády k občasnému zesvětlení místností,
- světelné scény.

Zastínění a žaluzie:

- časově nastavitelné zastínění místností,
- regulace rozptýleného světla nastavením lamel žaluzií podle intenzity slunečního svitu a zamezení přímé sluneční radiace,
- nastavení zimního a letního režimu:
    - v létě proti přehřívání místností,
    - v zimě k maximalizaci doby přímé sluneční radiace,
- automatické svinutí vnějších žaluzií při nárazech větru.

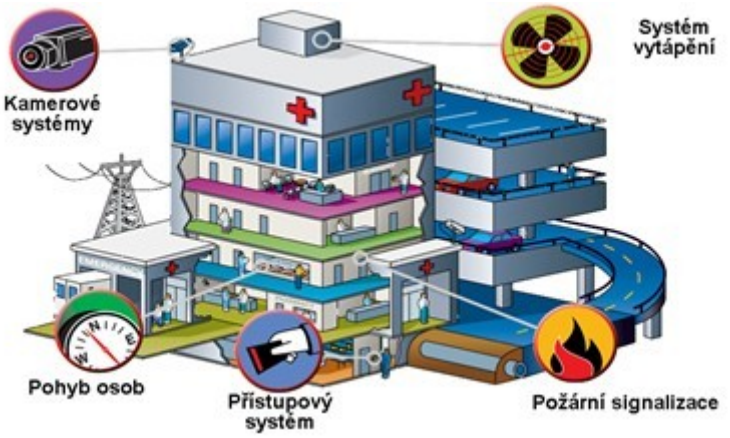
Bezpečnost:

- vyznačení únikových cest při požáru,
- snímač kouře v místnostech vydá při zakouření pokyn k odvětrání elektricky nastavitelnými okny,
- v případě požárního poplachu se na obrazovkách kancelářských počítačů objeví únikový plán,
- vyhlášením poplachu se sepne domovní osvětlení,

- simulace přítomnosti osob k řízení osvětlení,
- kontrola vstupu osob v přístupovém prostoru buď systémem Key-Card, nebo snímáním biometrických údajů.

Multimédia:

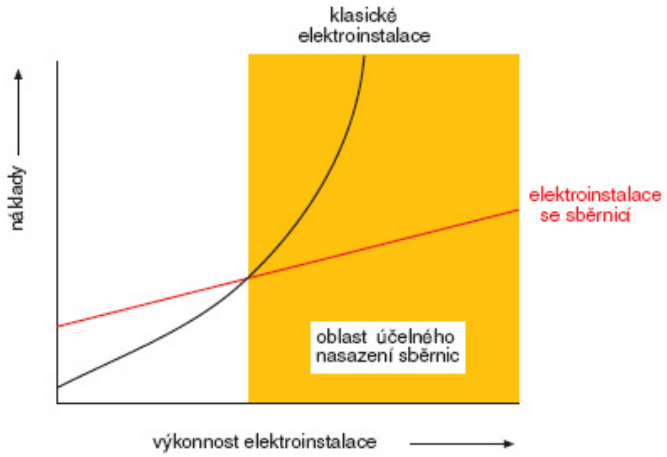
- aktivace světelné scény při zapojení projektoru při prezentaci,
- ovládání vybavení místnosti systémem Personál Digital Assistent (PDA), mobilním telefonem anebo PC. [1].



Obr. 6 Budova s integrovanými systémy

2.9. Standardizované sběrnice a sítě v automatizaci budov

Základním předpokladem pro integraci všech technických zařízení do uceleného systému v jedné budově je komunikační propojení. Již ve středně veliké správní budově se mezi automatizačními místy a centrálním nadřízeným počítačem předává na tisíc různých informací. Tuto funkci již po řadu let řeší systém sběrnic (Bus System). Klasickou elektroinstalací by bylo možné zajistit většinu požadavků, kladených na elektrické vybavení budov. Při rozsáhlejších instalacích, zajišťujících velké množství požadovaných úkolů, stoupají však neúměrně náklady na elektroinstalaci a od jisté výkonnosti se vyplatí přejít na sběrnicový systém (obr. 1).



Obr. 7 Závislost nákladů na výkonnosti elektroinstalace

V dnešní době již každá moderní budova obsahuje různé technologie, které zajišťují komplexní řízení a správu celé budovy. Tyto technologické systémy automatizace budov využívají různé komunikační protokoly.

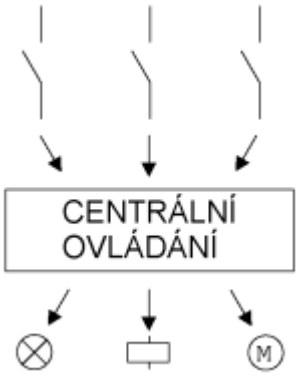
Systémy automatizace budov byly v minulosti přebírány z průmyslové automatizace. Za tuto dobu byla vytvořena řada standardů, v systémech automatizace budov byly vytvořeny první komunikační standardy teprve v druhé polovině 80. let. V roce 1990 byl pak na evropské úrovni ustanoven technický výbor, který pro automatizaci budov vybíral sběrnice ze stávajících standardů. V následující částí popisuji základní technické parametry komunikačních sběrnic a protokolů využívaných v systémech automatizace budov. Detailněji budou popsány následující protokoly: EIB/KNX, Modbus, EcheLON, Mbus a BACnet. Vzhledem k tomu, že v následujícím textu budou velice často používány pojmy komunikační sběrnice a protokol, uvedu definice několika pojmů [3].:

Protokol: soubor pravidel pro komunikaci mezi dvěma nebo více uzly (systémy, regulátory).

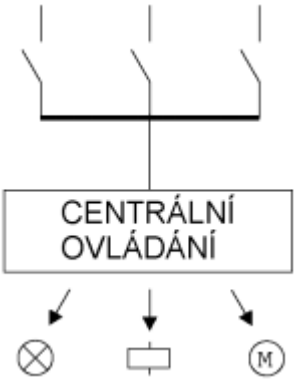
Sběrnice: (anglicky: Bus) je skupina signálových vodičů, kterou lze rozdělit na skupiny řídicích, adresových a datových vodičů v případě paralelní sběrnice nebo sdílení dat a řízení na společném vodiči (nebo vodičích) u sériových sběrnic. Sběrnice má za účel zajistit přenos dat a řídicích povelů mezi dvěma a více elektronickými zařízeními. Přenos dat na sběrnici se řídí stanoveným protokolem.

Centralizovaný systém: U centralizovaného systému (ovládání elektrických spotřebičů) jsou vstupy (spínače, tlačítka, senzory, apod.) a výstupy (svítidla, spotřebiče, aj.) propojeny s centrálním řízením hvězdicově. To znamená, že každý účastník (senzor, případně spotřebič) má vlastní spojení s centrálním řízením a centrálou, se kterou vzájemně komunikují. Toto uspořádání je obvyklé například u programovatelných automatů (PLC).

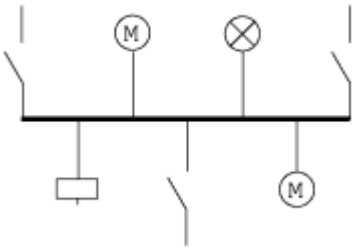
Hybridní (částečně decentralizovaný systém): tady jsou vstupy (senzory) zapojeny na sběrnici, zatímco výstupy jsou hvězdicově připojeny na řídící jednotku.



Obr. 10 Centralizovaný systém



Obr. 9 Hybridní systém



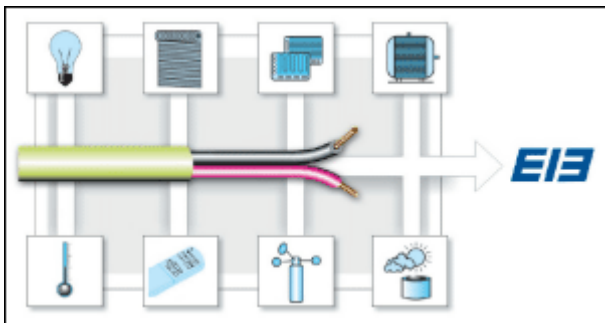
Obr. 8 Decentralizovaný systém

Decentralizovaný systém: O decentralizovaném systému mluvíme, má – li každý účastník (senzory i aktory) vlastní „inteligenci“ (mikroprocesor s vlastní pamětí). Každý účastník je přímo připojen na sběrnicové vedení. Mluvíme o „decentralizované inteligenci“, kdy neexistuje žádné centrální řízení a zaručena větší spolehlivost provozu (např. EIB, LON, aj.). [3].

2.9.1. Sběrnice EIB

Evropská instalační sběrnice EIB (European Installation Bus) vznikla z elektroinstalační sběrnice Instabus firmy Siemens. Sběrnice EIB má decentralizovanou strukturu s liniovou, kruhovou nebo větvenou topologií. Maximální délka jedné větve/linky je 1000 m a může k ní být připojeno maximálně 64 zařízení. Informace po sběrnici jsou předávány v tzv. telegramech (zprávách). Pomocí liniových spojek lze k páteřní síti připojit až 12 větví. Liniové spojky pak zajišťují, aby telegram putoval jen do té větve, pro kterou je určen. Důležitým signálům může být přidělena vyšší priorita a tyto jsou pak upřednostňovány (rychlejší postup celou sítí, kratší odezva). Systém EIB je otevřený pro všechny další obory, avšak primárně je určen pro elektroinstalaci. Pomocí signálových vodičů jsou jednotlivá zařízení propojena a také napájena.

Programování jednotlivých účastníků a celého systému EIB se provádí počítačem pomocí programu ETS (EIB Tool Software). Jako základní přenosové médium je použito krouceného páru vodičů (označováno jako EIB-TP). Dále může být použito síťové vedení (EIB-PL - Power Line) nebo přenos signálů rádiem (EIB-RF - Radio Frequency). Výhodou sběrnice je ta, že mohou být bez problému propojovány zařízení různých výrobců.



Obr. 11 Příklad decentralizované struktury sběrnice EIB

Jednoduchost zařízení využívající sběrnici EIB zaručuje především bezproblémovou instalaci a uvedení do provozu. Montáž, instalaci a nastavení zařízení tak jednoduše zvládne vyškolený elektroinstalatér. V procesu nastavování parametrů systému se zadáním příslušných adres určí, který snímač má dané akční členy ovládat. Přiřazení snímačů lze jednoduchým přeprogramováním kdykoliv změnit a tedy je možné elektroinstalaci přizpůsobit změnám dispozic bez jakéhokoliv fyzického zásahu do elektrické instalace. [3].

2.9.2. Sběrnice KNX

Jako základ pro mezinárodní standard KNX byla zvolena sběrnice EIB pro její technický charakter i úspěch na trhu (bylo již realizováno přes sedmdesát tisíc projektů).

Obr. 12 Logo protokolu

Hovořily pro ni v zásadě tři výhody EIB:

- kompatibilita výrobků různých firem,
- jasná certifikace,
- jednotné uvádění do provozu (EIB-Tools).

Veškeré výrobky a zařízení určené pro sběrnici EIB vyhovují automaticky standardu KNX (a často bývají současně označovány oběma ochrannými známkami EIB a KNX). Standard KNX má oproti EIB mnohem větší objem funkcí, odpovídající požadovanému cíli, a to spojení nejrůznějších přístrojů. Možnost využití dalších přenosových médií, integrace různých zařízení (pro vytápění, větrání, klimatizaci a různých domácích spotřebičů), ale i nové druhy uvádění do provozu umožňují propojení automatizace budov s automatizací domácností do skutečného "inteligentního" domu. Vytvořením standardu KNX se dostalo evropské sběrnici EIB mezinárodního zhodnocení.

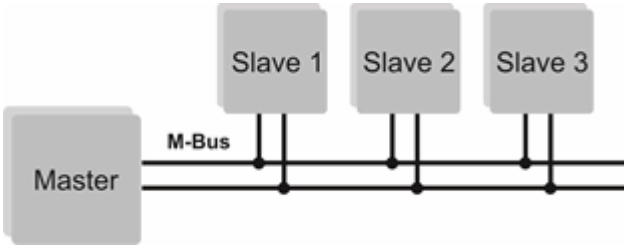
V současné době existuje již řada výrobců, kteří zařazují do svých výrobních programů přístroje pracující na sběrnici KNX/EIB, čímž se tento systém stává stále cenově dostupnějším. Z těch nejvýznamnějších budu jmenovat například firmy GIRA, MERTEN, ABB, Siemens, které se systému KNX/EIB věnují již řadu let a velkou měrou přispěli k rozšíření systému nejen do celé Evropy, ale i na světový trh.

Adresování a programování jednotlivých komponentů se provádí pomocí softwarového nástroje ETS3.0, kdy pro každý sběrnicový prvek existuje tzv. produktová databanka, která v sobě obsahuje aplikační program. Tyto databanky poskytují většinou volně ke stažení přímo výrobci komponent a po importu do ETS3.0, kde je možné aplikaci nakonfigurovat dle potřeby a takto upravený program instalovat zpět do zařízení. V současné době lze spoustu programování a nastavování provádět pomocí speciálního modulu po síti TCP/IP. [3].

2.9.3. Sběrnice M-Bus

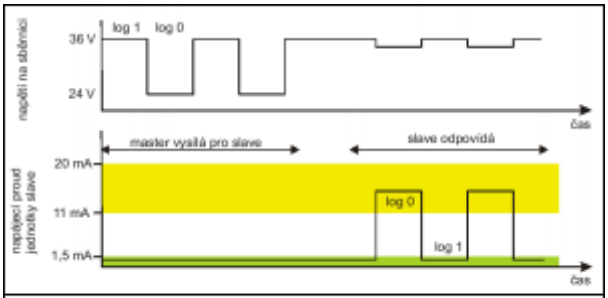
Sběrnice M-Bus (z anglického Meter-Bus) je určena pro aplikace sběru dat z měřičů odběru nejrůznějších médií (například pitné a užitkové vody, plynu, tepla, elektrické energie). Sběrnice musí zajistit propojení relativně velkého počtu zařízení (řádově několika set) na vzdálenost až několika kilometrů. Jejímu rozšíření napomohla snadná instalace – postačí dva vodiče, po kterých je přístroj většinou i napájen. Přenos dat musí být kvalitně zabezpečen proti chybám.

Sběrnice M-Bus pracuje dle struktury modelu ISO/OSI, která je rozdělena do jednotlivých protokolových vrstev. Nejvýše je postavena tzv. správcovská vrstva (management level) umožňující správu a řízení nižších vrstev, např. změnu komunikační rychlosti. Koncovou vrstvou je tzv. fyzická vrstva, která využívá výše zmiňované dvouvodičové vedení, které slouží zároveň jako napájení. Podřízení účastníci (slave) se na tuto dvouvodičovou sběrnici připojují paralelně (obr. 13).



Obr. 13 Komunikace na sběrnici M-Bus

Ke komunikaci z nadřízené jednotky (master) do jednotek slave je využita modulace napětí na sběrnici. Používá se dvojúrovňová amplitudová modulace, ve které logická jednička odpovídá jmenovitému napětí 36 V na sběrnici a při vysílání logické nuly nadřízená jednotka snižuje napětí na sběrnici o 12 V. Zbytkové napětí 24 V na sběrnici, slouží k napájení podřízených jednotek. Podřízené jednotky používají k vyslání odpovědi modulaci procházejícího napájecího proudu. Logická nula je reprezentována aktuálním procházejícím proudem, při vysílání logické jedničky zvyšuje jednotka slave svůj napájecí proud o 11 až 22 mA (obr. 14).



Obr. 3. Princip modulace užívaný fyzickou vrstvou sběrnice M-Bus

Obr. 14 Princip modulace fyzické vrstvy

Data na sběrnici M-bus jsou přenášena asynchronně s délkou 8 bitů a sudou paritou (sudý počet jedničkových bitů ve slově). Mezi jednotlivými znaky nesmí být časové mezery. Pro rozsáhlejší systémy je nezbytné přejít ke složitějším konfiguracím, kdy je celý systém rozdělen na tzv. zóny. Jednotlivé zóny se skládají ze segmentů připojených prostřednictvím vzdálených opakovačů a jsou řízeny tzv. řadiči zóny.

V praxi se tato sběrnice výlučně používá pro sběr dat z měřičů odběru médií. Nejčastěji se lze setkat s měřiči spotřeby tepla, průtočného množství, odběru plynu, apod. Zařízení jsou propojena k řídící jednotce a prostřednictvím koncentrátoru jsou data ukládána do počítače, kde mohou být dále zpracovávána.

Obr. 15 Sběr dat na sběrnici M-Bus

Komunikace mezi koncentrátorem a počítačem se uskutečňuje prostřednictvím sériové linky RS-232. Některé koncentrátory obsahují i optické rozhraní a je možné data vyčítat pomocí optické čtečky. Příklad sběru dat z jednotlivých měřičů do PC je uveden na obr. 15. [3].

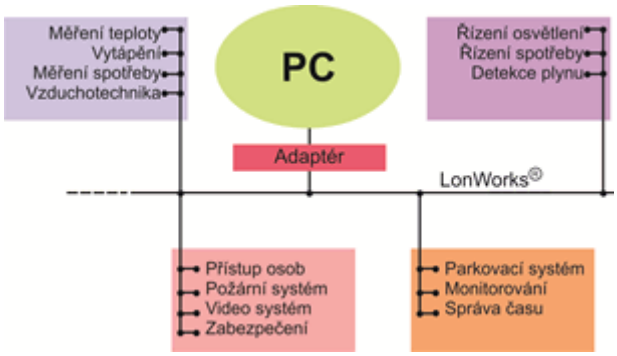
2.9.4. Sběrnice LON

Standard LON (Local Operating Network) byl vyvinut počátkem 90. let americkou firmou Echelon jako univerzální a levné komunikační spojení pro všechna možná technická použití na nejnižší automatizační úrovni.

Cílem byla výroba čipu s názvem Neuron, obsahujícího všechny potřebné funkce. Použitý protokol se nazývá LonTalk a celá technika se označuje souborně jako LonWorks. Topologie je odvozena z počítačových sítí.

Sběrnice LON je otevřený decentralizovaný sběrnicový systém využívající sériového přenosu dat (zpráv). Sestává z uzlů (řídicí systémy, regulátory), které si mezi sebou vyměňují informace. Každý regulátor obsahuje univerzální čip, obsahující neuronový čip a připojení na sběrnici.

Neuronový čip obsahuje tři osmibitové procesory, paměti, časovací jednotku, vstupní/výstupní část a komunikační sběrnici.



Obr. 16 Sběrnice LON

Digitální signál sběrnice LON je přenášen sériově ve tvaru zpráv (telegramů) na různých přenosových mediích: kroucené páry vodičů, elektrorozvodná síť, vysokofrekvenční rádiové vlny, infračervené spojení, koaxiální kabel a skleněná vlákna. Přenosová rychlost se pohybuje mezi 600 b/s až 1,25 Mb/s podle použitého média a délky spojení. U kroucených párů vodičů se na vzdálenost 2 700 m dosahuje rychlosti 10 kb/s, zatímco na vzdálenost 1500 m až 78 kb/s a na 130 m až 1 250 kb/s.

V systému LON použitý protokol LonTalk je částí firemního programu (firmware) a je dnes již otevřený (standardizován v EIA-709), takže jej lze implementovat i mikroprocesory nezávislými na čipu Neuron. EIA (sdružení Electronic Industries) tento standard reorganizoval a byl přejmenován na ANSI/CEA-709.1. Nicméně termín EIA-709.1 je dodnes často používaný.

V praxi se sběrnice LON s výhodou využívá v aplikacích, kde je kladen nárok na délku sběrnice (nikoliv na rychlost přenosu dat). Základní využití sběrnice je v případě propojování různých systémů (vytápění, CCTV, přístupové systémy, řízení spotřeby energií, apod.). Pro připojení sběrnice LON do PC je nutné využít vhodného adaptéru. Adaptérem jsou data transformována ze sběrnice do příslušného vizualizačního systému, který umožňuje data zobrazit. [3].

2.9.5. Protokol BACnet

Komunikační protokol BACnet je především určený pro automatizační a operátorskou úroveň automatizace budov. Podstatou protokolu BACnet je formulace univerzálního popisu všech možných funkcí zařízení.

Protokol BACnet je celosvětovou normou, výkonným standardem automatizace budov. Používá se bez licenčních poplatků. Evropské a americké skupiny pracují na možnosti certifikace zařízení BACnet, aby byla zaručena zaměnitelnost produktů různých výrobců.

Obr. 17 Logo protokolu

Přenos zpráv protokolem BACnet lze realizovat několika různými způsoby:

- Prostřednictvím sítě Ethernet (BACnet/IP). V současnosti je tato komunikace v systémech automatizace budov nejvyužívanější. Přenos dat se na tomto přenosovém médiu pohybuje rychlostí 10MBps a 100MBps.
- Prostřednictvím sítě RS-485. Sběrnice RS-485 je sériová linka, typ protokolu Master-Slave/Token-Passing (MS/TP). MS/TP má jeden nebo více uzlů (MASTER), kteří spolupracují v logickém kruhu. Sběrnice může mít i účastnické uzly (SLAVE), které ovšem nemohou vysílat zprávy bez jejich vyžádání MASTERem.

Protokol BACnet specifikuje tři hlavní části:

- Definuje"OBJEKTY" jako datové body, požadované hodnoty, časové programy, kalendáře
- Definuje "SLUŽBY" jako sdílení dat, alarmy a správu událostí, časování, trendy, správu zařízení a sítě
- Definuje standardy komunikačních médií: BACnet přes Ethernet, BACnet přes LonTalk, BACnet přes RS232

Vzhledem k výše popsanému, je výhodné použití protokolu BACnet v aplikacích, kde se využívá komunikace po Ethernetu (internetového připojení). Některá zařízení, která mají implementovanou komunikaci po protokolu BACnet, mají integrovaný webserver a je tedy možné k těmto zařízením přistupovat zadáním odpovídající IP adresy. [3].

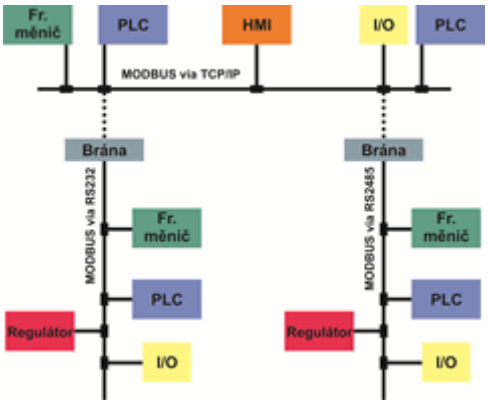
2.9.6. Protokol Modbus

Modbus je otevřený protokol vhodný pro vzájemnou komunikaci různých zařízení (programovatelné automaty, vstupně/výstupní zařízení, dotykové displeje), který umožňuje přenášet data po různých sítích a sběrnicích. Tento protokol má hlavní využití v průmyslových aplikacích, nicméně využití v systémech automatizace budov má také již své pevné postavení. Komunikace protokolu funguje na principu předávání datových zpráv mezi klientem a serverem (master a slave). Na sběrnici je jedno "master" zařízení (tedy jeden "klient", v případě verze Modbus TCP jich může být

více) posílající dotazy, ostatní zařízení jsou "slave" (tedy "server"). "Slave" zařízení odpovídá na dotazy, které jsou mu adresovány. V pozici mastr je tedy řídící prvek (např. PLC nebo průmyslové PC), v roli slave zařízení jsou ovládané nebo sledované prvky (např. čidla, měřicí přístroje, PLC, prvky výrobních linek apod.).

Obr. 18 Logo protokolu

Protokol MODBUS definuje strukturu zprávy na úrovni protokolu (PDU - Protocol Data Unit) nezávisle na typu komunikační vrstvy. V závislosti na typu sítě, na které je protokol použit, je PDU rozšířena o další části a tvoří tak zprávu na aplikační úrovni (ADU - Application Data Unit). Kód funkce udává serveru jaký druh operace má provést. Rozsah kódů je 1 až 255, přičemž kódy 128 až 255 jsou vyhrazeny pro oznámení záporné odpovědi (chyby). Některé kódy funkcí obsahují i kód podfunkce upřesňující blíže požadovanou operaci. Obsah datové části zprávy poslané klientem slouží serveru k uskutečnění operace určené kódem funkce. Obsahem může být například adresa a počet vstupů, které má server přečíst nebo hodnota registrů, které má server zapsat.



Obr. 19 Protokol ModBus

Přenosová média a verze protokolů:

- Ethernet přes TCP/IP
- asynchronní sériový přenos (RS-232C, RS-422, RS-485, optické vlákno, radiový přenos)

- MODBUS PLUS vysokorychlostní síť

Protokol preferuje sériovou komunikační sběrnici standardu RS485, preferovaný režim sériové linky je 19200 baudů, 8 datových bitů a sudá parita. Definuje dva sériové vysílací režimy, MODBUS RTU a MODBUS ASCII. Režim určuje, v jakém formátu jsou data vysílána a jak dekódována. Každá jednotka musí podporovat režim RTU, režim ASCII je nepovinný. Všechny jednotky na jedné sběrnici musejí pracovat ve stejném vysílacím režimu.

Jak už jsem zmínil, používá se tento protokol převážně v průmyslových aplikacích. V systémech automatizace budov se tento protokol využívá spíše pro integrace průmyslových zařízení do centrální stanice systému automatizace budov. Většina systémů v budovách dnes vyžaduje informace i z průmyslových zařízení (například z frekvenčních měničů, které ovládají čerpadla nebo pohony).

Z uvedeného přehledu komunikačních sběrnic a protokolů je patrné, že v současné době se v systémech automatizace budov využívá více sběrnic a protokolů. Je nutné poznamenat, že nebyly uvedeny všechny komunikační protokoly, které se v budovách využívají (např. SNMP, C-bus, Nikobus, apod.). Popsány ovšem byly ty nejvíce používané. V systémech automatizace budov se v současné době nejvíce prosazují sběrnice EIB/KNX, LON a BACnet. V menších projektech se používají levnější individuální řešení. Většinou je na projektantovi a dodavateli, kterou komunikační sběrnici navrhne a použije. Je pak na příslušném technikovi (programátorovi), jakým způsobem provede komunikaci vybraných sběrnic a protokolů. Zvláště obtížná je situace v případě integrace systémů využívajících jiný druh komunikačních protokolů. Na tyto integrace již dnes ale existuje řešení v podobě řídicího integračního systému (softwarové nebo hardwarové řešení). Sběrnice EIB je jednoznačně evropská, s poměrně přehlednou topologií srozumitelnou i pro zaškoleného elektroinstalatéra; sběrnice LON naproti tomu typicky americká a je možné ji počítačově ovlivňovat. [3].

2.10. Integrace systémů a komponent používaných pro automatizaci budov

V předchozích odstavcích jsem představil pouze základní přehled sběrnic a komunikačních protokolů pro systémy automatizace budov. Je zřejmé, že zdaleka nebyly uvedeny všechny protokoly, které systémy automatizace budov využívají. Využití komunikačních protokolů je závislé na technologiích a systémech instalovaných v budovách a požadavku komunikace mezi jednotlivými systémy. V dnešní době již nezávisí na tom, zda se jedná o budovu administrativní, průmyslovou nebo rodinný dům. Současné trendy totiž neustále vyžadují použití nejnovějších technologií. Hlavní požadavek je dnes kladen na integraci jednotlivých systémů, tedy předávání hodnot různých veličin z jednoho systému do systému druhého. Uvedu některé technologie, systémy a komponenty včetně

možností integrace systémů v závislosti na využití různých systémů automatizace budov a komunikačních protokolů. Uvedeny budou možnosti integrace systémů na úrovni softwarové (nadstavby v PC) a procesní. [4]

Obr. 20 Možné propojení komunikačních protokolů

2.10.1. Integrace řídicích systémů a technologií

Téměř všechny nově postavené nebo zrekonstruované moderní budovy již v dnešní době obsahují propracované řídicí systémy. Hlavním úkolem těchto systémů je automatizované řízení v rámci dané technologie. Navržené technologie, které jsou instalované v moderních budovách, je nutné vhodným způsobem ovládat a také zobrazovat. V případě využití více systémů instalovaných v jedné budově je také nutné systémy vhodně sjednotit tak, aby si jednotlivé systémy mezi sebou předávaly potřebné informace. Jelikož je dnes možné využít celou řadu moderních systémů, jako jsou například systémy: vytápění (HVAC), zabezpečení, protipožární ochrany, řízení elektrických rozvodů, osvětlení, přístupu osob a informačních technologií, je nutnost integrace technologií čím dál více aktuální. Nehledě na to, že uvedené technologie většinou využívají různé komunikační protokoly.

Nejčastěji používanými komunikačními protokoly jsou EIB/KNX, Modbus, EcheLON, Mbus, BACnet, OPC a SNMP. Není tedy možné jednoduchým způsobem propojit různé technologie s různými komunikačními protokoly. Téměř vždy musí být použit odpovídající adaptér nebo převodník, který je instalován do řídicího počítače. Řídicí počítač obsahuje systém správy budov (BMS - Building Management System) a zprostředkovává komunikaci mezi různými protokoly. V reálné aplikaci to pak může vypadat tak, že řídicí počítač (server obsahující BMS) je mnohdy nestabilní a může docházet k výpadkům předávání informací mezi jednotlivými technologiemi. V současné době existuje mnoho BMS umožňujících ovládání integrovaných technologií a tyto systémy jsou převážně instalované na řídicím počítači (PC) a je tedy nutné vždy brát ohledy na bezpečnost komunikace, stabilitu těchto systémů (po delší době nutnost upgrade), složité nastavení a instalaci použitých převodníků a konfiguraci celého BMS systému.

Obr. 21 Integrátor a regulátor

Jak bylo výše naznačeno, integraci systémů je možné vytvořit využitím zásuvných karet (obsahující převodníky) nebo adaptérů, které jsou připojené do řídicího PC. Řídicí PC pak obsahuje odpovídající systém správy budov, jehož součástí jsou příslušné ovladače a vytváří tak grafickou vizualizaci nad integrovanými technologiemi. Druhou možností integrace technologií je využití regulátoru, který v podstatě nahrazuje PC.

Obr. 22 Propojení komunikačních protokolů systémem HAWK

Takovýto regulátor obsahuje potřebné fyzické vstupy a výstupy (převodníky a adaptéry jsou součástí systému) a umožňuje integraci připojených technologií, vytváření řídicí logiky a grafickou vizualizaci celého systému. Díky tomuto systému je pak možné jednoduchým způsobem integrovat různé technologie, které komunikují různými komunikačními protokoly (viz obr. 22). Navržený regulátor tak jednoduchým způsobem umožňuje integraci technologií s různými komunikačními protokoly. Pro integraci komunikačních protokolů je nutné pouze zvolit příslušný ovladač a regulátor je následně připraven na integraci dané technologie. Zvolením požadovaných datových bodů (parametrů) může systém operovat s daným bodem a předávat jeho hodnotu do jiné technologie, která třeba komunikuje po jiném komunikačním protokolu. Vybrané regulátory mohou obsahovat konektory pro připojení LAN (TCP/IP a BACnet) a konektory pro připojení sériové linky RS232 a RS485. Dále je možné systémy libovolně doplnit o další komunikační rozhraní LON, Modbus, Mbus, EIB, apod. Dle uvedených komunikačních rozhraní je patrné, že některé systémy umožňují v jednom zařízení používat několik komunikačních protokolů najednou. Využitím komunikačních protokolů je pak možné předávat hodnoty vybraných veličin z jednoho systému (např. přístupový systém) do systému druhého (např. vytápění). Díky těmto informacím může systém aktivovat vytápění v dané místnosti, budově až po přiložení přístupové karty některého zaměstnance. Takovýto systém se pak významně

podílí na snížení vydané energie v budově. Díky tomu se pak regulátory stávají plnohodnotnými systémy pro integraci současných technologií v moderních budovách. [4]

2.11. Bezpečnostní systémy

V další části se již budu zabývat jen určitým odvětvím automatizace budov, zaměřeným na bezpečnostní systémy, a to konkrétně na systémy kontroly vstupu a přítomnosti osob. Také se zmíním o perimetrické ochraně objektu a o integrovaném kamerovém systému.

2.11.1. Systémy kontroly vstupu

Moderní budovy se neobejdou bez přístupového a zabezpečovacího systému. Integrací těchto systémů do BMS systému získáme větší přehled o dění v budově a zvýšíme celkovou úroveň zabezpečení. Přístupové systémy jsou velmi efektivním nástrojem pro elektronickou kontrolu vstupu do objektů, místností, vjezdů do garáží, parkovišť, průjezdů vrátnicí a identifikaci osob.

- ✓ Nepotřebujete klíče - stačí jen Váš otisk prstu nebo jedna identifikační karta pro všechny dveře.
- ✓ Otisk prstu neztratíte a identifikační kartu v případě její ztráty zneplatníte jediným kliknutím.
- ✓ Můžete připojit systém k internetu a z libovolného PC nastavit povolení vstupu do objektu.
- ✓ Můžete kontrolovat, kdo a kdy vstupuje do Vašeho objektu.

Obr. 23 Čtečka otisků prstů TLR401

Správce systému má tak přehled, kdo se po budově pohybuje. Pomocí karet s přístupovými právy je zajištěno to, že se lidé pohybují jen tam, kde mohou. Řídící jednotka umožňuje velmi efektivně ovládat rovněž výtahy a turnikety. Pomocí jedné karty může zaměstnanec vjíždět na parkoviště, procházet zabezpečenou budovou nebo nakupovat v místním občerstvení. Propojením lze docílit významných úspor nákladů na energie v budově. Systém reaguje na různé druhy vstupů. Uvedu následující příklad: Při vstupu prvních zaměstnanců ráno do budovy musí tito zaměstnanci použít svou

kartu pro umožnění vstupu. Systém to zaregistruje a dá informaci BMS systému, že má začít topit, dle venkovního světla nebo hodnotě osvětlení v kanceláři zapne či vypne uvnitř světla, seřídí žaluzie dle venkovních podmínek apod. V případě odchodu posledního zaměstnance z kanceláře, systém automaticky vypne světla a sníží hodnotu vytápění nebo klimatizace na úsporný režim. Výhodou integrovaného přístupového a zabezpečovacího systému je také možnost nastavení vyšší úrovně kontroly přístupu. V provozech, kde se pracuje s důvěrnými daty, cennými předměty, nebezpečnými materiály apod. je mnohdy důležitá kontrola pohybu osob. Funkce systému Anti-Passback (ochrana proti zpětnému průchodu) zabezpečí prostory tak, že každá osoba se musí prokazovat na vstupu i výstupu do různých zón v budově svou vlastní přístupovou kartou, jinak se nedostane do další zóny nebo zpět. V případě, že projdou dvě osoby na jednu kartu, osoba, která svou kartu nepoužila při vstupu, se již nedostane nikam jinam a ostraha objektu je upozorněna varovnou hláškou na monitoru, že se někdo pokoušel o nepovolený vstup.

Pro větší zajištění bezpečnosti v budově i okolí je možné systém propojit s CCTV kamerovým systémem a elektrickou a požární signalizací. Tímto propojením mohou bezpečnostní složky v budově okamžitě reagovat na poplachy ze zabezpečovacího systému a tyto poplachy zkontrolovat kamerovým systémem. Rovněž se mohou automaticky otevřít únikové východy v případě požáru apod. [8].

2.11.2. Kompatibilita v rámci systému

Je důležité, aby čtečky a karty, vybrané k použití v rámci jediného systému, pocházely od stejného výrobce. Používají se často přístupové karty a čtečky od společností HID, Indala a Idesco. Výrobek každé značky se dodává v řadě provedení, které zajistí plnou kompatibilitu se systémy. K uspokojení potřeb uživatelů slouží několik různých technologií. Patří k nim nejmodernější smart karty a biometrické přístroje, ale také tradičnější výrobky jako je Wiegand, Proximity (bezkontaktní prvky) a Magnetic Stripe (prvky s magnetickým proužkem). [8].

2.11.2.1. Technologie Smart karet

Smart karta – je to plastová karta s vestavěným čipem, která splňuje funkce kontroly přístupu paměti a produkci řady specifických funkcí. Důležitá odlišnost smart karty spočívá v tom, že provádí nejen uložení, ale i zpracování dat obsahujících informace. Obsah čipu karty je důkladně chráněn od cizího přístupu. Je to jedna z hlavních výhod smart karty.

Existují tři typy smart karet:

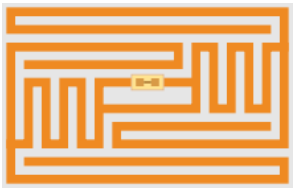
- ✓ kontaktní,
- ✓ bezkontaktní,
- ✓ hybridní (s dvojitým rozhraním).

Kontaktní smart karta se skládá se tři části:

- ✓ čip s integrovaným obvodem (mikrořadič karty),
- ✓ plastový podklad
- ✓ kontaktní oblast.

Kontaktní oblast obsahuje 6 nebo 8 kontaktů čtvercového nebo oválného tvaru. Velikost plastového podkladu karty a umístění kontaktů jsou určeny Mezinárodní organizací standardizace a odpovídá standardu.

Bezkontaktní smart karty jsou v dnešní době nejvíce perspektivním typem karet. Využívá se technologie radiofrekvenční identifikace RFID (Radio Frequency Identification). Smart karta obsahuje vestavěnou do těla karty indukční anténu a čip s integrovaným obvodem. Pro lepší mechanickou ochranu čip s integrovaným obvodem je umístěn do drobného bloku, který se připojuje ke koncům antény. Vestavěný integrovaný obvod se skládá ze dvou dílů – bezkontaktního radiofrekvenčního (RF) rozhraní a mikrořadiče. Obvod RF rozhraní je připojený na výstup antény smart karty a používá střídavé elektromagnetické pole emitované snímatelem pro získání napájecí energie pro smart kartu a pro výměnu dat mezi kartou a snímatelem [5].



Obr. 24 RFID čip s anténou

Karta hybridní s dvojitým rozhraním má současně kontaktní plochu a vestavěný induktor. Takové karty umožňují realizovat práce s různými typy snímatelů.

Snímatel generuje elektromagnetické záření určité frekvence. Při vnášení karty do zóny působení snímatelů, elektromagnetické záření zapojí čip karty přes vestavěnou anténu a RF rozhraní. V okamžiku správné identifikace přepošle do snímatele svoje identifikační číslo pomocí elektromagnetických impulsů určité frekvence.

Bezkontaktní smart karta funguje při vzdálenosti od 10 cm do 1 m v závislosti od pracovní frekvence snímatelů a nepotřebuji přesné centrování, což zaručuje jejich stabilní práci, pohodlí při využití a vysokou přenosovou schopnost. [8].

2.11.2.2. Biometrické systémy

Biometrické systémy nyní prochází rychlým vývojem a v budoucnosti se stanou velmi běžné. Tyto systémy jsou výhodnější než stávající zařízení, protože jejich pomocí lze lidi identifikovat podle nezaměnitelných znaků. Může se jednat o otisky prstů, snímky oční sítnice, profil obličeje nebo hlasu.

Jak pracují biometrické systémy?

Zařazení uživatele do systému (enrollment):

- ✓ sejmutí potřebných charakteristik a vytvoření referenčního profilu (vzorku)
- ✓ zpracování měření, extrakce nejdůležitějších charakteristik, vytvoření a uložení šablony (template)
- ✓ uložení šablony v identifikační databázi (ve vazbě na určitý identifikátor)

Ověření totožnosti - identifikace:

- ✓ aktuální měření - snímání daných charakteristik
- ✓ zpracování výsledků
- ✓ vyhledání šablony v databázi podle identifikátoru přiřazeného uživateli a porovnání s aktuálním měřením
- ✓ zaznamenání výsledku porovnání a následná akce - verifikace uživatele při shodě aktuálního měření s profilem nebo odmítnutí pro nedostatečnou shodu

Výhody biometriky:

- ✓ silná metoda - jak pro autentizaci samotnou, tak z hlediska obrany proti zneužití
- ✓ možnost kombinace s hesly nebo zdvojení více biometrických metod pro zvýšení spolehlivosti (pro kritické systémy)
- ✓ odolnost vůči krádežím nebo monitorování (na rozdíl od hesel nebo karet)
- ✓ uživatel se nemusí obávat ztráty karty nebo zapomenutí hesla či PIN

Nevýhody biometriky:

- ✓ složitost a náročnost na prostředky (technické i finanční) pro snímání a porovnání snímaného údaje s mnoha uloženými údaji v databázi
- ✓ nutnost zabezpečení identifikační databáze
- ✓ různá chybovost - chybné přijetí (nesprávné ztotožnění uživatele se vzorkem někoho jiného) nebo chybné odmítnutí (neztotožnění uživatele s jeho vlastním vzorkem).

Biometrická data by mohla v podnicích nahradit hesla nebo PIN, která se obtížně pamatují. Ještě kvalitnějšího zabezpečení je však možné docílit kombinací všech metod autentizace, protože tak se využijí všechny tři pilíře bezpečnosti: co máme (kartu), co známe (PIN) a co jsme (např. otisk prstu). [6].[8].

2.11.2.3. Technologie Proximity (bezkontaktní)

Jedná se o bezkontaktní vysokofrekvenční systém, který zajišťuje komunikaci mezi kartami / přívěsky na klíče a samotnou čtečkou. Čtečka vytváří vysokofrekvenční magnetické pole, kterým se do karty dodává energie potřebná k přenosu dat mezi jednotlivými prvky systému. Použitím různých čteček lze dosáhnout čtecích vzdáleností od 20 mm až do 1 m. [8].

2.11.2.4. Technologie Wiegand

Technologie Wiegand se opírá o dobře zavedenou normu a využívá speciální krátké vodiče, které se zapouští do karty. Vodiče jsou vyrobeny ze speciální slitiny s magnetickými vlastnostmi, které se obtížně napodobují. Sada drátků může obsahovat data, jako jsou čísla kreditních karet, čísla bankovních účtů, identifikační údaje zaměstnance, a jiné. Kartu přečteme průchodem přes nebo umístěním do blízkosti snímače Wiegand. Tato technologie nabízí střední až vysokou úroveň zabezpečení. Výroba karet Wiegand trvá déle, než výroba většiny ostatních karet. Vlastnosti těchto

karet, jako rychlá doba odezvy a přesnost, široký rozsah teplot pro možnosti použití, dělají Wiegand karty a čtečky ideální pro použití v terénu. [8].

2.11.2.5. Technologie magnetických proužků

Technologie magnetických proužků je nejjednodušší a nejtradičnější formou řízení přístupu. Vzhledem k rostoucím nárokům na zabezpečení ztrácí tato technologie na oblibě. Funkce karty závisí na magnetickém proužku umístěném na zadní straně karty, která se musí čtečkou protáhnout.

Magnetický proužek má tři záznamové stopy, které mají specifický účel:

- ✓ Stopa 1- První stopa má 79 znaků, které obsahují číslo karty (až 18 číslic) a jméno klienta (až 26 alfanumerických znaků).
- ✓ Stopa 2- Druhou stopu vyvinula American Bankers Association (ABA) pro on-line finanční transakce. Tato stopa obsahuje 40 numerických znaků včetně čísla karty (až 19 číslic) a v bankovnictví se používá nejvíce.
- ✓ Stopa 3- Tuto stopu vyvinuly banky pro finanční transakce. Na rozdíl od 1. a 2. stopy, které jsou určeny pouze pro čtení, může být záznam na 3. stopě přepisován. [8].

2.11.2.6. Multitechnologické přístupové karty

Současným trendem pro řešení přístupových karet je slučování různých typů přístupových karet do jediného modelu, jenž tak nabídne podporu pro více služeb. Dosavadní vývoj probíhal tak, že se nejprve používala jako přístupová karta bílá plastová karta s grafikou, logem firmy, případně fotografií pro vizuální identifikaci např. při vstupu do budovy, při kontrole na vrátnici apod. Tato identifikace však byla velmi málo bezpečná, bylo možné si takovou kartu pořídit na tiskárně plastových karet.

Prvním prvkem elektronické identifikace, osob nebo zboží ve skladech, bylo použití čárového kódu. Můžeme říct, že začalo elektronické zpracování dat. Jednoduchý terminál se čtečkou čárových kódů na vrátnici již zaznamenal osobu podle ID a porovnal s databází osob zavedených předtím do paměti terminálu. Neoprávněným osobám takové karty znemožnily přístup například přes turnikety do areálu pracoviště apod. Výhodou tohoto elektrického zpracování byla i kontrola docházky, odchodu či příchodu a následně mohla být zaznamenána data pro vypracování mzdy. Nevýhodou čárových kódů je však opět možnost jejich falšování, a to buď možnou kopií čárového kódu (na obyčejné kopírce) nebo např. označením při odchodu ze zaměstnání kolegou apod.

Na vyšší bezpečnostní úrovni pak bylo použití magnetického proužku na plastové kartě. Tento začaly využívat zejména banky pro zápis šifrovaných dat na platební karty. Ty jsou v bankách používány dodnes, ale spíše jen z důvodu přechodu na bezpečnější kartu Visa.

Již před více než dvaceti lety se začaly používat karty s kontaktem, které měly jednoduchou konstrukci čipu, většinou paměťového, a nebyly příliš bezpečné (telefonní automaty). Dnes jsou k dispozici dva druhy čipových karet – paměťové a mikroprocesorové. Paměťové karty mohou uchovat určité množství dat a patří mezi ně třeba ISO karta obvykle s 255 bity úložného prostoru. Mikroprocesorové karty, známé jako smart karty, představují inteligentní karty, které obdobně jako PC mají paměť, centrální procesorovou jednotku a jednotku pro komunikaci. Existují dva základní typy smart (inteligentních) karet s mikroprocesorem: kontaktní a bezkontaktní. Oba mají mikroprocesor vnořený do karty, bezkontaktní verze nemají zlatem pokrytý kontakt viditelný na kartě.

Bezkontaktní karty jsou dvojího typu:

- pracující na frekvenci 125 kHz, jsou buď pasivní, nebo aktivní a jejich společným znakem je identifikace pomocí čísla, které se ve čtečce pouze načítá. Ostatní řeší software na základě tohoto čísla. Obsahují anténku, pomocí které dochází ke komunikaci vzduchem. Nazývají se také proximity karty.
- pracující na frekvenci vyšší – 13,56 MHz, jsou rychlejší a jsou zapisovatelné, a to podle určitého systému. Například Mifare ®1KB karty mají 16 sektorů vždy po čtyřech blocích a ten každý po 16 bytech. Poslední dva bloky slouží k nahrání klíčů (A, B). Karty iClass mají 32 bloků s tím, že obsahují pole pro S/N, konfigurační data, klíče a aplikace HID. Počet a obsah vlastních aplikačních oblastí je pak dán velikostí paměti. Např. karta iClass 2K/2 obsahuje 2K paměti a dvě aplikační oblasti. Technologie bezkontaktních čipových karet HID iClass (13,56 MHz) určených pro čtení zápis, optimalizovaná pro dokonalejší zajištění kontroly vstupu osob, může být použita i pro ukládání biometrických otisků a dalších užitečných údajů. Kdykoliv můžete přidat nové aplikace bez nutnosti vydávání nových identifikačních karet.

Obr. 25 Multitechnologická karta

Na obrázku č. 25 je příklad karty, která v sobě slučuje všechny výše uvedené možnosti. Taková karta je žádaná ve firmách a institucích, kde byly postupně zaváděny různé systémy s kartami, a dnes je trend využít jediné tzv. multitechnologické karty, kterou lze použít jak pro stávající systémy,

tak pro nové, mnohem bezpečnější přístupy. Multitechnologická karta může obsahovat čárový kód, magnetický proužek, bezkontaktní čipy na obou frekvencích a kontaktní čip s inteligencí (mikroprocesorem). Navíc takováto karta může obsahovat řadu vizualizačních a ochranných prvků včetně hologramů. Tímto vznikne velmi výkonné a cenově efektivní řešení.

Velice důležitou podmínkou pro výrobce je dodržování mezinárodních standardů. Pro kontaktní karty platí norma ISO 7816-1 až 4, která definuje kontaktní kartu a komunikaci s ní. Čtení dat a konverze na třeba Wiegand, C&D (Clock&Data) či RS485 jsou také specifické pro čtečky a výrobce. Každý výrobce má navíc svoje specifická řešení pro autentizaci karty, přístup do paměti i pro čtení dat a jejich vazbu na vlastní čtecí systémy. Pro ty většinou standardy/normy neexistují, různí výrobci je řeší po svém. Významnou součástí takovýchto řešení je pak i šifrování při přenosu dat a vazba na čtečku. V současné době se významnou měrou rozšířily bezkontaktní karty s technologií využívající vysokou frekvenci 13,56 MHz, která díky výrazně vyšší rychlosti komunikace (až 848 Kb/s) dovoluje přenášet i větší objemy dat. Tato vlastnost podstatně zvýšila bezpečnost karet, které tak jsou schopny provádět vzájemnou autentizaci s čtečkou, šifrovat, ukládat a chránit data.

Obr. 26 Příklad použití multitechnologické karty

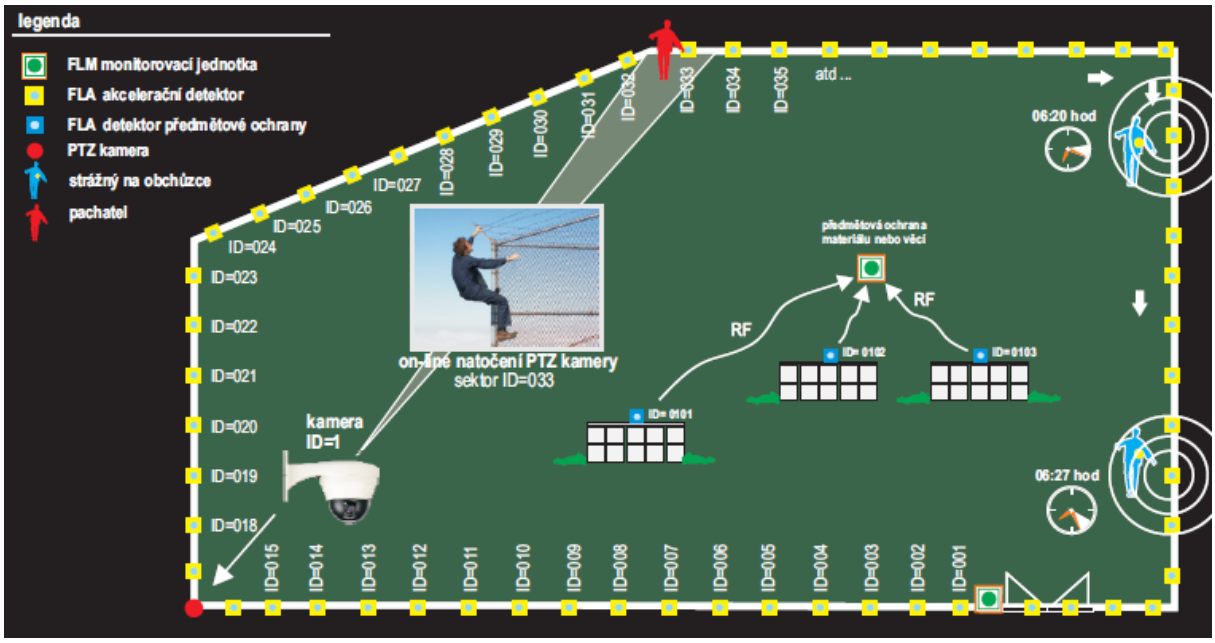
Nejrozšířenější komunikační standard pro vysokou frekvenci RFID je ISO/IEC 14443 (karta Proximity) umožňující čtení na vzdálenost maximálně 10 cm, a dále pak standard ISO 15693 pro karty Vicinity komunikující na delší vzdálenost – až do 1 metru. Největší celosvětový výrobce bezkontaktních karet, firma HID Global, dodává i kartu, která kombinuje výhody obou standardů – pro komunikaci například na parkovišti využívá ohledně čtení na dlouhou vzdálenost model Vicinity, a pro další aplikace, kdy držitel je blízko čtečky, pak Proximity. [7]

3. Analýza a návrh řešení systému kontroly pohybu osob

Po teoretické části, kde jsem se snažil vysvětlit principy a fungování problematiky moderních instalací a rozebrat možnosti jednotlivých hlavních protokolů a standardů nejpoužívanějších sběrnic, se budu dále zabývat jednou z částí systému – bezpečnostními systémy. V předchozích pasážích jsem vybral a popsal některé systémy a část jich použiji v mém návrhu komplexního zabezpečení kontroly vstupu do areálu administrativní firmy dle požadavků investora. Záměrem investora bylo omezit závislost najaté bezpečnostní agentury, která prováděla své služby střežením objektu a areálu vrátnými. Tato varianta začala být z jejich pohledu poměrně neefektivní a finančně náročná. Alternativou by mohlo být právě zautomatizování určitých činností.

Dle těchto požadavků jsem nejprve navrhl perimetrickou ochranu s kontrolou vjezdu do areálu. Areál je celý oplocený s jedinou vstupní bránou a zastaralou nefunkční závorou. Po řádné prohlídce a proměření se dohodlo na zachování stávající kovové brány, která vyhovuje požadavkům a po patřičném ošetření nátěrem bude sloužit danému účelu. Následně bude vybavena dvěma pohony s bezpečnostními prvky. Nefunkční závora se demontuje a nahradí novou a moderní. Obě zařízení se budou ovládat automatizovaně, a to brána pomocí bezdrátovými vysílači a GSM ovládačem a závora bezkontaktními kartami. Veškerá technická specifikace je popsána v přiloženém n8vrhu technické zprávy. Tyto automatizované funkce budou integrovány do systému, který byl zadán jako další požadavek, a to kompletní kontrolu pohybu osob v kancelářské budově. V této budově je předpokládaným účelem pronájem kancelářských prostor cizím firmám a na tomto základě, včetně bezpečnostního hlediska, bylo vytvoření systému kontroly přístupu. Byl použitý systém českého výrobce identifikačních systémů TECHFASS s centralizovanou správou a sběrem dat, který zaručuje dobrou integritu s jinými systémy. Systém se bude skládat z čtecích modulů MREM63 125kHz s integrovaným kontrolérem pro jedny dveře, které budou ovládat elektrické zámky ve vstupech, rozdělených hierarchicky do jednotlivých skupin. Hlavní vstup do budovy bude mít nejvyšší prioritu, následovat budou vstupy na jednotlivá patra a třetí skupinou kancelářské místnosti. Takto lze dosáhnout vhodného rozčlenění a variability dispozic a oprávnění. Nezbytnou součástí a také z bezpečnostního hlediska, budou společné prostory (vstup, schodiště, chodby) monitorovány CCTV IP kamerami včetně nahrávání. Kamera bude sledovat i vstupní bránu jako kontrolu přístupu do areálu. Veškeré tyto bezpečnostní prvky budou napojeny na stávající EZS.

Součástí zabezpečení je i dříve zmíněná perimetrická ochrana, navržena RFID bezdrátovým systémem střežení plotu a vrat „PERIMETR LOCATOR®“. Je to perimetrický systém umožňující střežení plotu pomocí speciálních akceleračních RFID detektorů (tagů) připevněných na plotě a vratech. RFID detektory nevyžadují napájení a životnost jejich baterií je cca 8 let. Systém je certifikovaný do nejvyšší 4. kategorie zabezpečení objektů.



Obr. 27 Přehledové schéma

Po tomto seznámení s návrhem části bezpečnostních systémů jsem zvolil další pokračování diplomové práce jako zpracování technické dokumentace a to konkrétně návrhu technické zprávy, která konkrétně popisuje požadavky investora, na jejímž základě byla vytvořena jednotlivá technická řešení včetně technických specifikací, montážních postupů a odkazů, schémat zapojení. V poslední části je zpracovaná kalkulace tohoto návrhu a porovnání se současným stavem.

3.1. Návrh dokumentu „Technická zpráva“

3.1.1. Základní údaje

Projekt řeší napojení a instalaci bezpečnostních a vstupních systémů v areálu firmy a v kancelářské budově.

3.1.2. Rozsah projektové dokumentace

Dokumentace řeší:

- navržení automatizace vstupní brány a závory včetně ovládání
- navržení systému kontroly vstupu na jednotlivé podlaží a jednotlivé kanceláře včetně monitoringu CCTV
- navržení systému perimetrické ochrany prostoru areálu RFID technologií

Dokumentace neřeší:

- silovou elektroinstalaci (osvětlení, zásuvky)
- ochranu před bleskem – vnější i vnitřní
- elektroinstalace v dalších přilehlých objektech

3.1.3. Podklady pro projektovou dokumentaci

3.1.3.1. Stavební výkresy

Výpis z katastrální mapy

Projekty stavební a elektroinstalace

3.1.3.2. Normy ČSN

ČSN EN 50090 Elektronické systémy pro byty a budovy (HBES)

ČSN EN 55022 ED2 Zařízení informační techniky – Charakteristiky rádiového rušení – Meze a metody měřen

ČSN EN 55024:1999 Zařízení informační techniky – Charakteristiky odolnosti – Meze a metody měření

ČSN EN 61000 Elektromagnetická kompatibilita (EMC)

ČSN EN 50065 Signalizace v instalacích nízkého napětí v kmitočtovém rozsahu 3 kHz až 148,5 kHz

ČSN EN 60065 Zvukové, obrazové a podobné elektrotechnické přístroje – Požadavky na bezpečnost

ČSN EN 61508 Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností

ČSN EN 60335 Bezpečnost elektrických spotřebičů pro domácnost a podobné účely

ČSN EN 60950 Zařízení informační technologie - Bezpečnost

ČSN EN ISO 16484 Automatizační a řídicí systémy budov

ČSN EN 50083 Kabelové distribuční systémy pro televizní a rozhlasové signály

ČSN EN 12453 Vrata - Bezpečnost při používání motoricky ovládaných vrat

ČSN EN 12445 Vrata - Bezpečnost při používání motoricky ovládaných vrat - Zkušební metody

3.1.3.3. Požadavky investora

3.1.3.3.1. Automatizovaný pohon vstupní brány

Automatizovaný pohon vstupní brány ovládaný identifikační kartou nebo dálkovým ovládáním, kde brána by měla zůstat stávající. Při ranním příchodu, jedním z určených zaměstnanců,

se brána otevře a zůstane otevřená až do konce pracovní doby, kdy opět určený zaměstnanec bránu uzavře a tím zabezpečí celý areál. V průběhu pracovní doby bude fungovat jako kontrola vjezdu automobilů automatická závora, ovládaná taktéž identifikačními kartami.

3.1.3.3.2. Přístupový systém v kancelářské budově

Hlavním požadavkem investora bylo zajištění kontroly osob s oprávněním k různým dveřím kanceláří a vstupy do jednotlivých pater v komerční kancelářské budově. Celý chod systému bude monitorován IP kamerami ve vstupu a na chodbách, kamery v kancelářích nejsou požadovány. Autorizace a identifikace osob pomocí karet bude programována a spravována na centrálním počítači.

3.1.3.3.3. Perimetrická ochrana plotu a vrat

Dalším požadavkem bylo zabezpečení perimetrické ochrany areálu, s podmínkou provedení bezdrátovým systémem bez použití nebo omezení kabelových rozvodů z důvodu ekonomické a technické náročnosti.

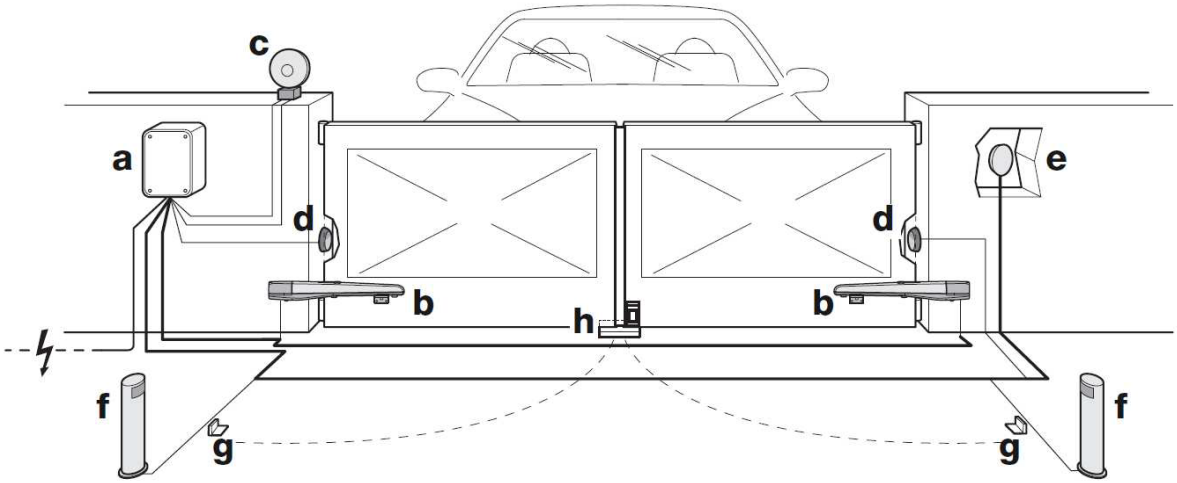
3.1.3.4. Katalogy výrobců

Technopark CZ s.r.o. – katalogové listy, montážní návody, propagační materiály
AZ – Pohony s.r.o. - katalogové listy, montážní návody, propagační materiály
TechFass s.r.o. - katalogové listy, montážní návody, propagační materiály
7 Marsyas Development a.s. - katalogové listy, montážní návody, propagační materiály

3.1.4. Popis technického řešení

3.1.4.1. Pohon a ovládání vstupní brány

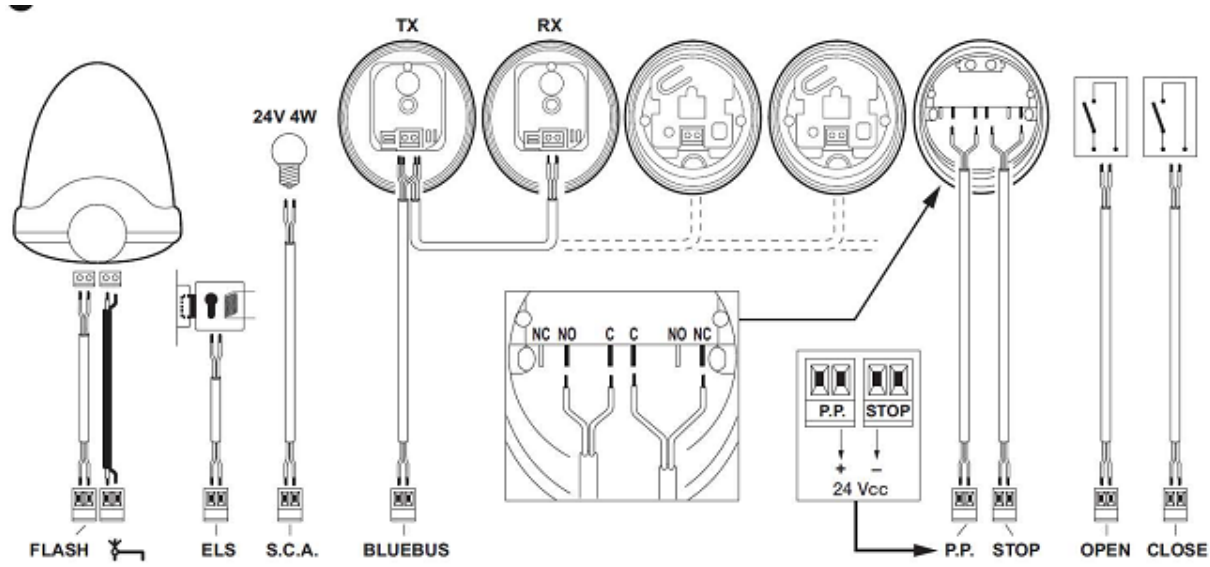
Dle požadavku investora bude využita stávající dvoukřídlová brána, široká 6 m, kovové konstrukce s pevnými kovovými sloupky. Návrh uvažuje o použití pohonu firmy TECHNOPARK, typ Toona. Jedná se o nadzemní pohon pro křídlové brány do 7 m, pro naši bránu použijeme řadu TO5000. Pohony jsou v principu ve dvou verzích – 230 V a 24 Vdc. Použijeme verzi s napájením 24V.



Obr. 28 Situační schéma a rozmístění komponent

Před samotnou instalací je potřeba zkontrolovat rozměry a hmotnost křídla brány, zda nepřekračují mezní hodnoty z grafu 1 [*příloha I*]. Dále podle grafu 2 [*příloha II*] vypočtěte vzdálenost pro umístění zadní konzoly, upravte a namontujte na označené místo. Podobně postupujte u přední konzoly. Montáž konzol je dána přesnými rozměry, aby byl zaručen přímý pohyb automatizační techniky a brána se otevírala ve správném úhlu. Pokračujeme montáží pohonu a seřízení koncového spínače. Automatizaci pohonů a ovládání bude řídit digitální jednotka MC824H, která zaručuje bezpečnost a spolehlivost. Pro elektrickou instalaci budou použity kabely CYKY a JY(ST)Y dle tabulky 1 [*příloha III*], chráněné v instalační trubce. Do stávajícího asfaltového povrchu budou vyřezány drážky pro instalační trubky, průchod v prostoru mezi komunikací a budovou se uloží do výkopu 50 cm hlubokého, v chráničce až do rozváděče RVZ. Napájecí přívod pro zařízení bude veden kabelem CYKY – J 3x4 z rozváděče RP, který je situován v 1PP m. č. 018 do podružného rozváděče RVZ umístěného na venkovní zdi objektu. Z RVZ bude veden napájecí kabel CYKY – J 3x1,5 do řídící jednotky. Veškeré obvody se zapojí prostřednictvím komunikačního systému Bluebus firmy NICE dle schématu a návodu. Tento systém umožňuje dvouvodičové elektrické připojení, po kterém se přenáší jak napájecí napětí, tak komunikační signály. Připojení jednotlivých zařízení se provádí paralelně a bez ohledu na polaritu. Během procedury „učení“ řídicí jednotka postupně rozpoznává jednotlivá připojená zařízení prostřednictvím specielně vyvinutého přenosového protokolu. Pokaždé, když je přidáno nebo smazáno nějaké zařízení, je nezbytné znovu spustit proceduru „učení“ řídicí jednotky. Nejprve připojte kabel napájecího přívodu a potom kabely od motorů M1a M2 a nakonec připojte kabely od různých zařízení systému. Aby byla řídicí jednotka schopna rozpoznat zařízení k ní připojená po sběrnici Bluebus, musí mít tato zařízení přiřazeny své adresy. Tato operace musí být provedena správným nastavením elektrických propojek (jumperů), které jsou součástí každého ze zařízení Bluebus. Viz manuály od jednotlivých zařízení. Poté provedeme iniciační spuštění, kdy na základě blikání LED diod jak na řídicí jednotce, tak na fotobuňkách a majáku, určíme správnost zapojení. Po tomto testu následují procedury načítání a nastavování motorů a poloh brány, a to buď

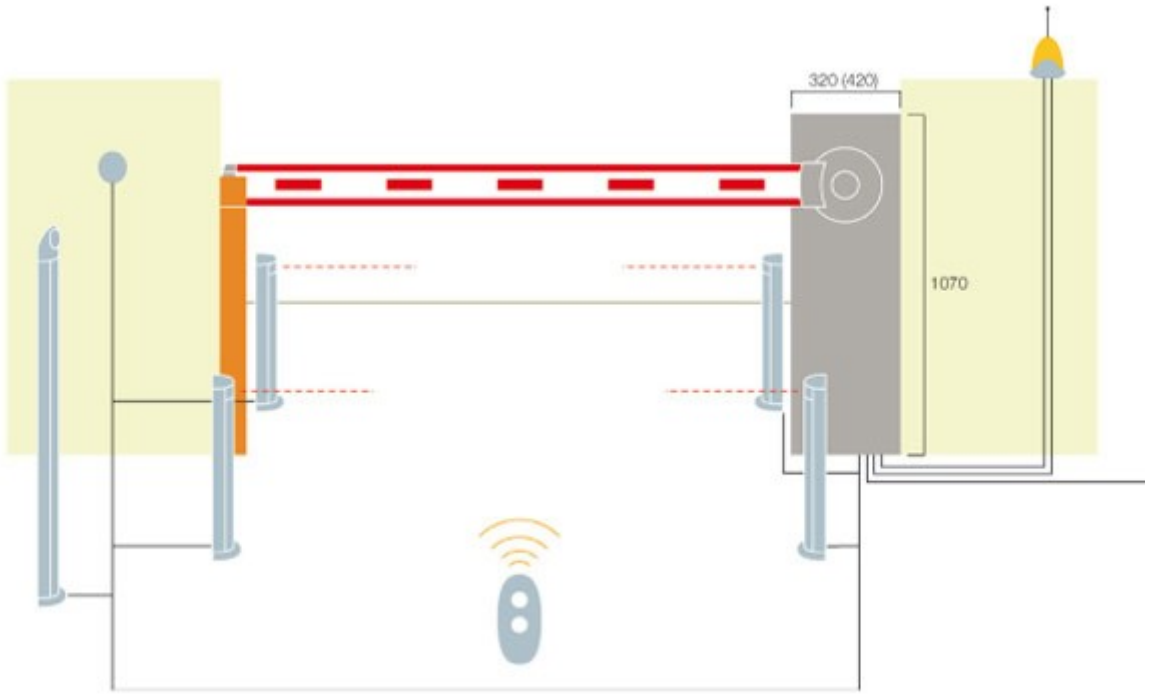
v automatickém nebo manuálním režimu. Nejdůležitější fáze instalace, na kterých závisí spolehlivost a bezpečnost zařízení je testování a uvedení do provozu. Tyto operace může provádět pouze kvalifikovaná osoba, která má k provádění těchto úkonů oprávnění dle platných předpisů. Zkoušky musí být provedeny podle normy EN 12445. Připojená zařízení musí být taktéž podrobena specifickým funkčním zkouškám v součinnosti s řídicí jednotkou MC824H [*příloha III*].



Obr. 29 Připojení ostatních zařízení

3.1.4.2. Automatická závora

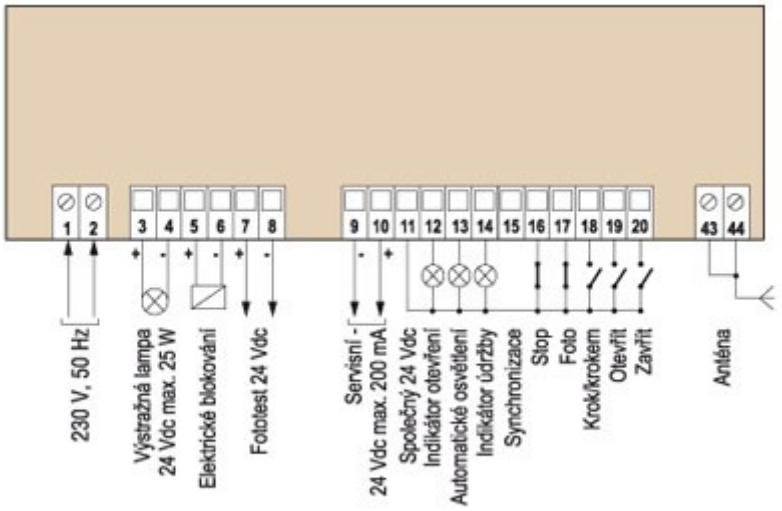
Pro použití je navržena elektromechanická závora 24 V DC, typ SIGNO 6, která plně vyhovuje požadavkům investora. SIGNO je elektromechanická závora skládající se ze základové desky, konzoly na připojení ramena závory a ovládací jednotky. Automatický systém je navržený pro dosažení koncových poloh (otvírání a zavírání) se zpomalovací fází, s monitorováním zatížení motoru během pohybu. Díky těmto kontrolním systémům všechny překážky, na které závora narazí v prostoru zdvihu, se okamžitě identifikují a způsobí obrácení směru pohybu (funkce průběžného snímače). Systém se dá používat v „ručním“, „poloautomatickém“ a „automatickém“ režimu pomocí funkcí jako je „Zavřít 0 sekund po FOTO“, „Vždy zavřít“ a dvěma typy signalizování semafory. Řídící jednotka je vybavena počítadlem cyklů pro plánování servisních zásahů a konektorem pro zasunutí přijímače SM. Závora se bude uzavírat ihned po projetí přes fotočlánek, otevírat se bude na základě identifikace kartou přes čtečku.



Obr. 30 Situační schéma závory

Ovládací jednotka budeme napájet kabelem CYKY-J 3x1,5 z rozvaděče RVZ z okruhu 2. Kabel bude zaústěn do ochranné trubky, uložené v zemi ve vyřezané drážce v chodníku. Kabely pro bezpečnostní maják a elektrický zámek použijeme typ JYTY 4x1 a protáhneme je v trubce, pro nízkonapěťové zařízení použijeme slaboproudé kabely JY (ST) Y. Po zapojení všech komponent a zařízení provedeme celkovou kontrolu, změříme napětí na svorkách, zkontrolujeme LED diody na vstupech (aktivní zařízení), dále zkontrolujeme všechna bezpečnostní zařízení, zda fungují správně (nouzové vypnutí, fotobuňky, aj.). Nakonec zkontrolujeme správnost pohybu ramene. Následují programování a nastavení mechanických dorazů, tento postup je nutný, protože řídící jednotka SIA20 musí změřit vzdálenost, kterou projde převodový motor, aby přemístil rameno ze zcela zavřené polohy (pozice 0) do zcela otevřené polohy (pozice 1). Podrobný postup nastavení je popsán v příloze 3.

Nakonec následuje nejdůležitější operace, která zajistí maximální bezpečnost a spolehlivost automatického systému. Postup testování se může používat pro periodické kontroly zařízení, které tvoří automatický systém. Testovaní celého systému musí provádět kvalifikovaný a zkušený personál, který musí stanovit, který test se bude provádět na základě příslušných rizik a ověřit shodu systému s platnými předpisy, legislativou a normami, hlavně však s požadavky EU normy 12445, která stanovuje testovací metody pro automatické systémy pro závory smíšených přechodů pro vozidla a chodce.



Obr. 31 Schéma zapojení ovládací jednotky

3.1.4.3. Ovládání zařízení

Pro ovládání křídlové brány použijeme přijímač SMXI pracující na principu „plovoucího kódu“ firmy NICE. Charakteristické na této sérii je to, že rozpoznávací kód je u každého vysílače jiný a mění se po každém jednom použití. Na to aby přijímač poznal daný vysílač, je potřebné zapsat jeho rozpoznávací kód do paměti přijímače. Zapsaný do paměti („nakódovaný“) musí být každý vysílač („dálkový ovladač“), který má komunikovat s řídící jednotkou. Aby přijímač pracoval správně, je potřeba použít anténu správně naladěnou a to buď anténu typu ABF anebo ABFKIT. Na připojení je nutné použít koaxiální kabel 50 Ω (např. RG58). Jako vysílač jsem navrhl typ FLOR2R

Obr. 32 Přijímač SMXI

Obr. 33 Vysílač FLOR2R

Jako druhá alternativa je navržena profesionální jednotka GSM RTU5015. Je to kompletní zařízení v kovové krabičce, které je určeno pro profesionální použití jak v domácnosti, tak pro průmyslové aplikace. Otevírá brány a závory pouze na základě prozvonění, tedy zdarma z Vašeho mobilního telefonu. Otevírá pouze na čísla, která má uložena ve svém interním seznamu

autorizovaných čísel, ostatní čísla odmítne. Skvělou funkcí je možnost zabezpečení pohonu proti krádeži nebo vandalům. Nastavuje se přes SMS zprávy. Má paměť pro 60 autorizovaných telefonních čísel. (Příloha 5).

Obr. 34 GSM jednotka RTU5015

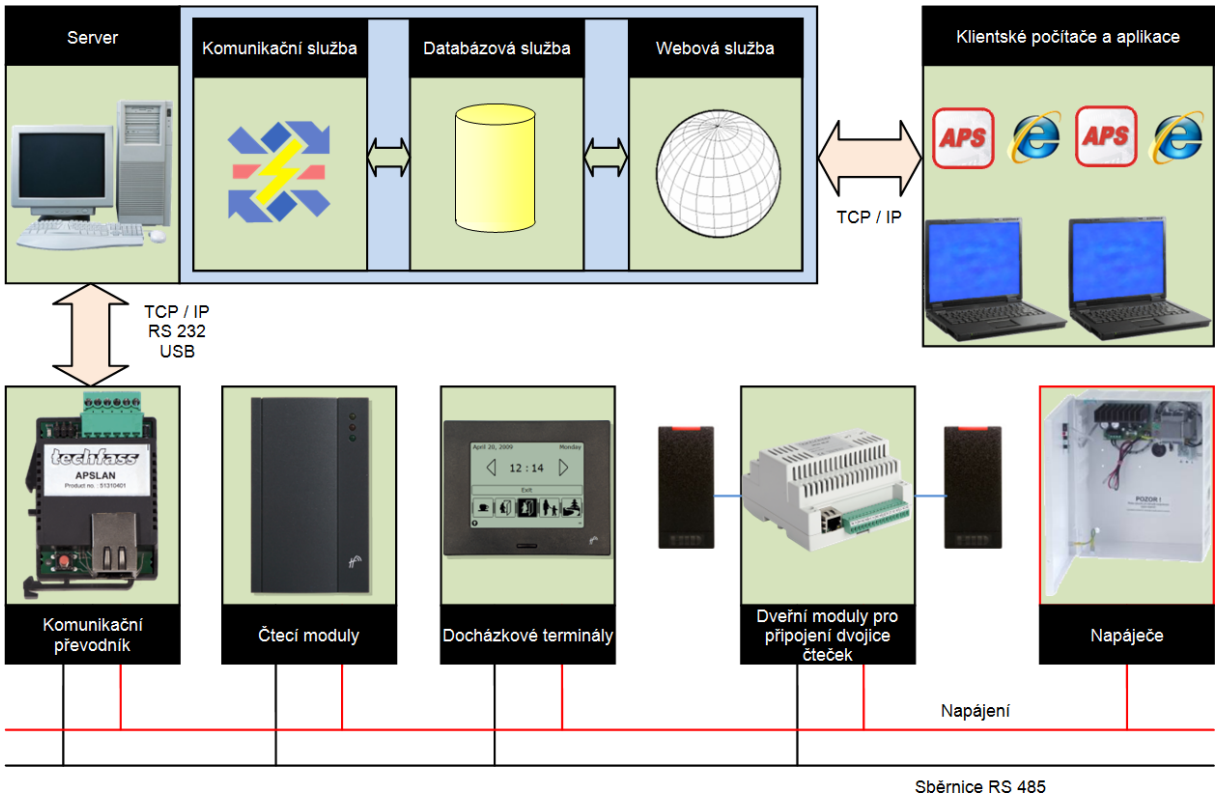
Ovládání závory je v našem systému navrženo dvěma čtecími moduly MREM 63 firmy Techfass, každý ve směru jízdy ze strany řidiče, upevněný na sloupku. Technické parametry jsou popsány v části přístupového systému níže. Komunikace a napájení bude zajištěno prostřednictvím komunikační linky RS 485, bude uloženo v trubce pod povrchem vozovky a napojeno na systém kontroly vstupu. **[***Příloha VI*].

3.1.4.4. Kontrola přístupu

Celý systém kontroly přístupu je založen na systému APS mini Plus od firmy TECHFASS, našeho předního výrobce identifikačních systémů. APS mini Plus je jednoduchý systém elektronické kontroly vstupu pro aplikace do 748 uživatelů. Základní funkci systému, tj. kontrolu vstupu a programování přístupových oprávnění, vykonávají čtecí moduly autonomně – bez nároků na jejich připojení k PC. V našem případě použijeme připojení k PC, kde lze přístupová oprávnění spravovat jednoduchým administračním programem a sledovat provozní události systému. Do tohoto systému budeme integrovat i jiná zařízení a systémy. Systém může pracovat v offline nebo online provozním režimu, kde probíhá komunikace s moduly permanentně. Provozní události systému jsou ihned vyčítány z paměti modulů a umožňují tak realizaci docházkových aplikací a dalších SW nadstaveb. Online připojení rovněž umožňuje vzdálené otevření dveří prostřednictvím PC.

3.1.4.4.1. Základní vlastnosti HW

- Pevně daná funkce, konfigurovatelné parametry
- Programování kartami nebo z PC
- 748 + 2 ID v paměti, $>10^7$ (online)
- Paměť pro 2000 událostí
- 32 modulů (adres) na lince, počet linek není omezen
- 64 časových plánů
- 64 svátků



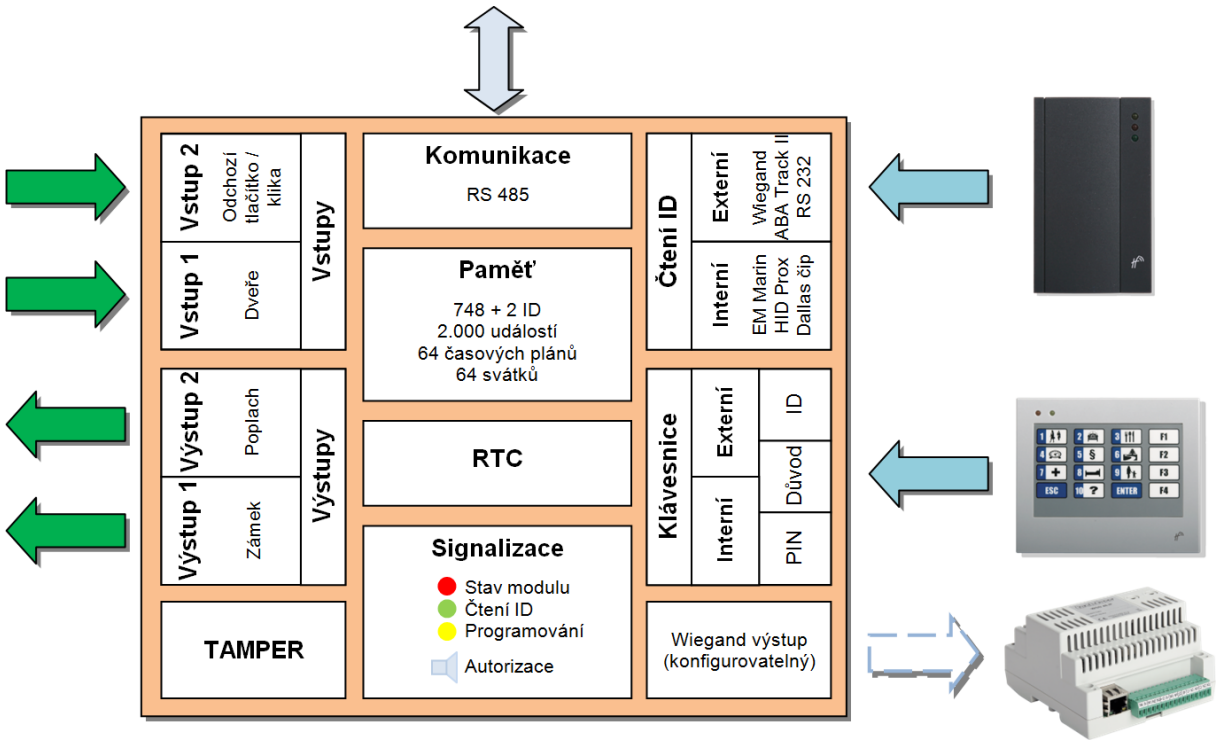
Obr. 35 Topologie systému APS Administrator

Pro správu přístupových oprávnění použijeme program APS Administrator. Toto řešení umožňuje kombinovat systém APS mini Plus se systémy APS mini i APS 400. Prvotní nastavení provozních parametrů modulu provedeme programem APS Reader.

Hardwarové moduly systému APS mini Plus vykonávají pevně danou funkci, jejíž parametry lze nastavit jednoduchým konfiguračním programem z PC. Moduly budou pracovat jako součást malého, centrálně spravovaného systému, propojeného prostřednictvím komunikační linky RS 485. Připojení linky k PC se bude realizovat prostřednictvím komunikačního převodníku RS485 - Ethernet (protokol TCP/IP). Každému čtecímu modulu budou prostřednictvím konfiguračního programu APS Reader nastaveny provozní parametry dle technické specifikace (viz příloha).

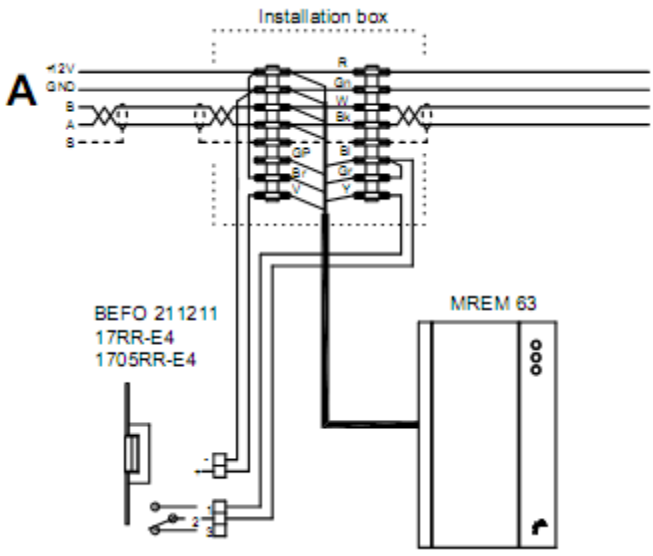
3.1.4.4.2. Systémové čtecí moduly

Systémové čtecí moduly jsou vybavené veškerými periferiemi pro zajištění funkce ovládání dveří (typicky 2 vstupy, 2 výstupy, 3x LED, bzučák, řídící logika), čtení ID médií (technologie dle typu integrované čtečky) a pamětí pro archiv událostí a přístupová oprávnění. Moduly jsou k dispozici v ucelené řadě mechanických provedení, vhodných pro nejrůznější typy montáže nebo vestavby do nejčastěji používaných designů modulárních systémů (např. bTicino, vstupní panely BPT apod.). Většina modulů obsahuje ochranné kontakty pro sledování neoprávněné manipulace s modulem. Moduly zajišťující vlastní čtení identifikačních médií disponují alternativním datovým výstupem WIEGAND, který umožňuje jejich použití ve většině identifikačních systémů, schopných pracovat se čtečkami s tímto standardním datovým rozhraním. Vlastní funkce modulu je potom redukována na čtení ID a jejich odesílání nadřízenému systému. Volbu provozního režimu modulu lze provádět uživatelsky, prostřednictvím programu APS Reader.



Obr. 36 Systém APS mini Plus

Pro připojení čteček jiných ID technologií (včetně biometriky) jsou k dispozici funkčně kompatibilní řídící moduly pro připojení čteček s výstupem WIEGAND, ABA Track II nebo RS 232. V našem systému jsou navrženy čtecí moduly MREM 63(čtečky 125kHz s integrovaným kontrolérem pro jedny dveře). Na jednu linku systému APS mini Plus je možné připojit až 32 čtecích modulů MREM 63. Počet linek není prakticky omezen. Použijeme verzi TF, která čte tovární ID media TECHFASS a HID Proximity. Technické parametry a vlastnosti jsou v příloze. ()



Obr. 37 Zapojení čtečky MREM 63

3.1.4.4.3. Instrukce pro montáž

Popis vodičů	Barva	Význam	Barva	Význam
	Rudá	Napájení +12 VDC	Zelenobílá	WIEGAND data 0
	Rudomodrá	Napájení +12 VDC	Hnědozelená	WIEGAND data 1
	Modrá	0 V	Žlutá	Vstup 1 (IN1)
	Zelená	0 V	Šedá	Vstup 2 (IN2)
	Černá	A vodič linky RS 485	Fialová	NO kontakt relé
	Bílá	B vodič linky RS 485	Hnědá	C kontakt relé
	Růžová	Poplachový výstup (AUX)	Šedorůžová	NC kontakt relé

Tab. 2 Popis vodičů čtečky

Std. zapojení		
	Vstup 1	Dveřní kontakt, při zavřených dveřích sepnut
	Vstup 2	Odchozí tlačítko nebo kontakt kliky, při stisknutém tlačítku nebo klice sepnut
	Výstup 1 (relé)	Ovládání zámku (konfigurovatelné)
	Poplachový výstup	Nízkoúrovňový tranzistorový výstup (+5 V při jakémkoliv poplachu)

Tab. 3 Popis svorek čtečky

Čtecí modul využívá pro svoji funkci pasivní RF/ID technologii, citlivou na vnější RF rušení. Toto rušení může přicházet buď vyzařováním okolního prostředí, nebo po napájecích vodičích. Je tedy nutné vyvarovat se montáži modulů v blízkosti možných zdrojů elektromagnetického pole, kterými mohou být například monitory počítačů (vzdálenost min. 3 m) nebo různé domácí a průmyslové elektrické spotřebiče. Rovněž je vhodné používat doporučené napájecí zdroje (lineární) pro omezení rušení přicházejícího po vodičích. Rušení způsobené vnějším polem je tím větší, čím více se jeho frekvence blíží pracovnímu kmitočtu čtecích modulů (125 kHz) a čím větší je jeho intenzita. Z tohoto

pohledu není zanedbatelné ani rušení čtecích modulů navzájem – pro správnou funkci je nutno dodržet vzdálenost minimálně 50 cm. Tuto vzdálenost mohou negativně ovlivňovat i různé metalické konstrukce (při pochybnostech je před konečnou montáží vhodné provést praktickou zkoušku na místě).

Vlastní montáž modulu se provádí pomocí vhodných hmoždinek přímo na nevodivou podložku. Po přimontování modulu na stěnu, nasaďte víko na horní část krabičky a otáčivým pohybem víko přiklopte, až zřetelně klapnou obě aretace. Z druhé strany zdi nebo ze strany vyššího zabezpečení (při oboustranné instalaci čteček) je třeba osadit montážní krabici pro připojení kabelů.

Nastavení modulu provádíme podle instrukcí v komunikačním programu APS Reader. Při zapojování čtecích modulů na sběrnici systému je třeba dodržet obecně platné zásady pro zapojování sběrnice RS 485. U modulů, kde se HW adresa nastavuje konfigurací jumperů, se nastaví adresa hned při montáži modulu (konfigurace je vždy uvedena v manuálu konkrétního výrobku). U ostatních modulů doporučuji zapsat si sériové číslo modulu do tabulky společně s HW adresou, kterou plánujete modulu přidělit (což vede ke značnému zjednodušení práce při dalším postupu).

Moduly, u kterých se nastavuje adresa hardwarově: xREM 56, xWGD 46(IP), xRRF 12,

Moduly, u nichž se nastavuje adresa softwarově: xREM (xREP, xRED) 53, xREM 55, xREM 63, xREM 57, MDEM 31(IP).

3.1.4.4.4. Provoz čtecích modulů

Čtecí modul zajišťuje následující funkce:

- Standardní funkci „Otevření dveří“.
- Sledování stavu dveří.
- Sledování stavu odchozího zařízení (tlačítka / kliky).
- Aktivaci poplachového výstupu při indikaci poplachového stavu.

Funkci „Otevření dveří“ lze aktivovat třemi různými způsoby:

- Načtením platného ID (karty, klíčenky).
- Stisknutím odchozího tlačítka (dle konfigurace).
- Softwarově, po komunikační lince.

V případě standardní funkce zámkového relé je po aktivaci funkce „Otevření dveří“ aktivováno uvolnění zámkového relé modulu a bzučák (pokud není konfigurací zakázán). Tento stav trvá do otevření dveří, nejdéle však do uplynutí doby nastavené parametrem „Doba aktivace zámku“. Poté je zámkový výstup deaktivován a standardní funkce ukončena.

V případě přepínací funkce zámkového relé je po aktivaci funkce „Otevření dveří“ aktivována změna stavu zámkového relé modulu a bzučák (pokud není konfigurací zakázán). Akustická signalizace uvolnění zámku trvá do otevření dveří, nejdéle však do uplynutí doby nastavené

parametrem „Doba aktivace zámku“. Stav zámkového relé zůstává nezměněn až do doby další aktivace funkce „Otevření dveří“.

Načtení ID v průběhu funkce „Otevření dveří“ hlásí modul po komunikační lince (v online režimu). V případě, že načtené ID není platné, je ohlášeno akustickým signálem „neplatné ID“ bez ohledu na konfiguraci akustického hlášení uvolnění zámku.

Při nastavení funkce „Trvalé uvolnění zámku dle časového plánu“ je v době platnosti příslušného časového plánu zámek trvale uvolněn, načtení platného ID je hlášeno po komunikační lince (v online režimu). V době trvalého uvolnění zámku nevzniká poplachový stav vyražené dveře.

Poplachové stavy modulu:

- Narušení (stržení z montážní podložky nebo demontáž víka krytu).
- Vyražené dveře.
- Dlouho otevřené dveře.

Poplachové stavy jsou hlášeny následujícím způsobem:

- Softwarově, po komunikační lince.
- Akusticky.
- Nastavením poplachového výstupu.

Poplachový stav „Narušení“ vzniká aktivací signálu Tamper při rozepnutí jazýčkového kontaktu uvnitř modulu (pokud je pod modulem instalován magnet MAG) nebo otevřením víka čtecího modulu (optoelektronický senzor).

Stav „Vyražené dveře“ vzniká po rozepnutí vstupu IN1 modulu bez předchozí aktivace funkce „Otevření dveří“. Jedinou výjimkou je otevření dveří při současně sepnutém vstupu IN2 modulu, který je nakonfigurován jako kontakt kliky.

Stav „Dlouho otevřené dveře“ vzniká otevřením dveří na dobu delší, než je povoleno v konfigurační tabulka.

3.1.4.4.5. Oživení a nastavení systému

Z hlediska HW splní požadavky jakýkoliv nový počítač, při použití staršího počítače je vhodné mít k dispozici alespoň následující množství operační paměti:

- OS MS Windows XP – 1GB RAM
- OS MS Windows Vista – 2 GB RAM

Doporučeným OS je MS Windows XP nebo novější OS od Microsoftu. Následuje nastavení portů a firewallu. Nainstalujeme program APS Reader a nastavíme převodník TCP/IP, v našem případě ASPLAN.

Konfigurace čteček:

Čtečky na komunikační lince jsou identifikovány svojí HW adresou. Tato adresa je v rozsahu 1-32, každá čtečka musí mít svoji unikátní adresu (některá zařízení (např. kontrolér MWGD46(IP)) zabírají na lince více než jednu adresu, konfigurací HW propojek je potom určena nejnižší adresa zařízení).

U čtecích modulů, u kterých se HW adresa nastavuje softwarově, je nutné nejprve nastavit parametry komunikace – COM port pro komunikaci přes sériovou linku nebo IP adresu a port pro komunikaci přes TCP/IP. Potom je možné nastavit HW adresy čtečkám jedním z následujících způsobů:

- Nastavení adresy pomocí sériového čísla čtečky – v programu APS Reader vyplňte na záložce „Zařízení“ v oblasti „HW adresa“ sériové číslo čtečky a zvolte požadovanou adresu. Po stisknutí tlačítka „Připojit“ si ověřte, že v levé části stavové lišty svítí nápis „Timeout“, který signalizuje, že na dané adrese programu neodpovídá žádná čtečka (je tedy neobsazena). Poté stiskněte tlačítko „Nastavit“, čtečce s daným sériovým číslem je nastavena požadovaná HW adresa.
- Nastavení adresy pomocí potvrzovacích ID – na záložce „Zařízení“ vyplňte kód známé karty do pole „Použití potvrzovacího ID“, zvolte požadovanou adresu a stiskněte tlačítko „Připojit“. Ověřte, že v levé části stavové lišty svítí nápis „Timeout“, který signalizuje, že na dané adrese programu neodpovídá žádná čtečka (je tedy neobsazena). Po stisknutí tlačítka „Nastavit“ se čtečky uvedou do stavu, kdy očekávají načtení potvrzovacího ID (zelenočervené střídavé blikání). Čtečka, na které je potom prezentováno zadané ID, získá požadovanou HW adresu.

Po nastavení HW adres všem čtečkám ověřte, že se program bez problémů komunikuje se všemi adresami na lince. Dalším krokem je nastavení parametrů pro ovládání dveří – všechny parametry naleznete na záložce „Zařízení“. Po nastavení těchto parametrů můžete program APS Reader opustit.

Nainstalujeme program APS Administrator a založíme databázi dle návodu. Dále nainstalujeme Program APS 400 nServer.NET a nakonfigurujeme. Tak máme připravený systém k nastavení administrace v programu APS Administrator.

Nejdříve nastavíme základní parametry, přihlašovací účty programu a přístupové skupiny a nakonec nainstalujeme mikročtečku pro přidávání karet do PC. Následuje vložení karet do databáze. To lze zajistit buď načítáním karet na mikročtečce, nebo načtením karet na jakémkoliv čtecím modulu v systému.

Po načtení přístupových karet vytvoříme osobní listy. Osobní listy budou vytvořeny do kořenového prvku organizační struktury (tuto strukturu si vybudujeme libovolně, na samotná přístupová oprávnění nemá žádný vliv). Příjmení uživatelů je nastaveno dle zadaného jména karty, při editaci lze všechny údaje opravit. Dalším krokem je rozdělení uživatelů do přístupových skupin – to je

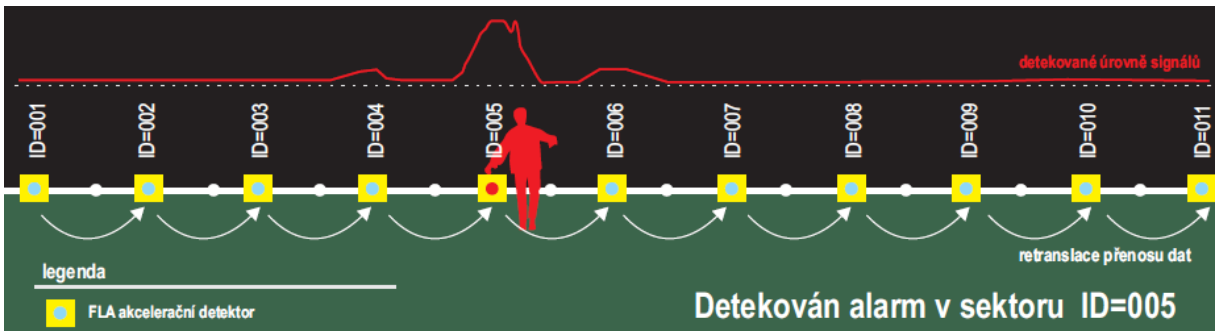
třeba učinit na záložce „Přístupové skupiny“ v editaci osobního listu. Tímto způsobem nastavte skupiny všem požadovaným uživatelům.

Nakonec provedeme přenos dat do systému. Dokončení procesu je signalizováno archivní značkou zapsanou do archivu událostí. Přenos dat je nutné spustit po každé změně přístupových oprávnění uživatelů v systému (do té doby je systém řízen poslední nahranou konfigurací).

Pro monitorování chodeb a vstupu byly navrženy IP kamery fy AVTECH, typ AVN222. Jde o barevnou dome IP kameru s kompresí H.264 a variobjektivem a pro venkovní vstup použijeme kameru AVN263ZP_12V - venkovní barevná IP-kamera s IR přisvětlením (40 metrů) a varifokálním objektivem. Napájení a přenos dat bude kabelem UTP, zdroj napájení bude umístěn do rozvaděče. Zpracování obrazu videa bude proveden v PC speciálním programem se záznamem.

3.1.4.5. Perimetrická ochrana plotu a vrat

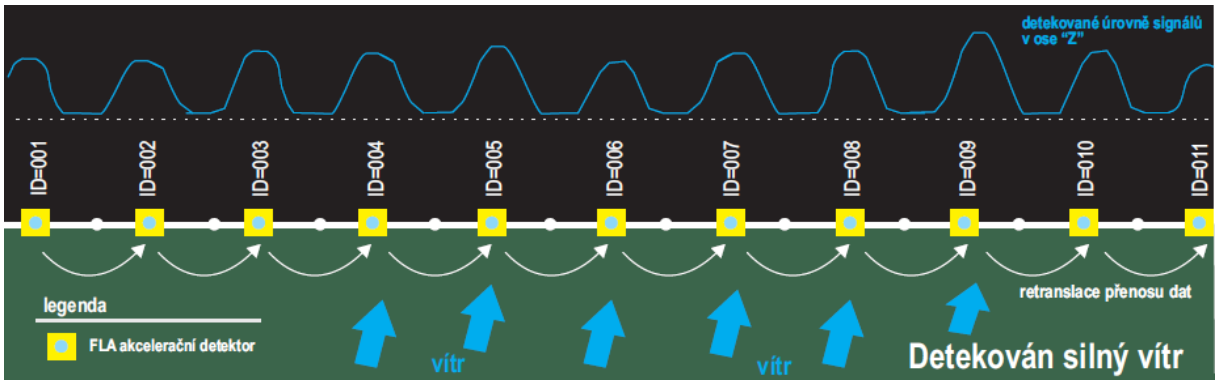
Jako ochranu před nezvanými návštěvníky je navržen bezdrátový perimetrický RFID systém (Perimetr Locator), který má proti konvenční (kabelové) instalaci nesporné výhody, akcelerační RFID detektory nevyžadují žádnou kabeláž, napájí se bateriemi s výdrží cca 8 let a jejích instalace je jednoduchá a rychlá. Je vhodný pro všechny typy plotů a vrat a má velmi vysokou odolnost proti rušivým klimatickým vlivům. Systém Perimetr Locator umožňuje realizovat také předmětovou ochranu střežení věcí uvnitř perimetru (chráněného prostoru) díky RFID detektorům. Tato funkce má svou výhodu a v případě potřeby je možno ji s výhodou využívat pro ochranu vozového parku a uskladněného materiálu. Samozřejmostí je komunikace se všemi typy EZS ústředen a v našem případě bude systém napojen na stávající EZS v hlavní budově. Taktéž systém poskytuje revoluční, naprosto přesné navádění průmyslových PTZ kamer na místo incidentu s přesností +/-3m. Tato funkce zatím zůstane nevyužita, ale v budoucnu se počítá s doplněním o kamery a posílením bezpečnosti prostoru.



Obr. 38 Princip detekce narušitel

Princip činnosti spočívá v tom, že se na jednotlivé dílce plotu nainstalují RFID detektory FLA, které pomocí 3osého akceleračního čipu detekují veškeré pohyby plotu. Jednotlivé detektory FLA mezi sebou komunikují na principu “tiché pošty”, tj. postupně bezdrátově přenášejí informace o alarmech, o

síle větru, sabotážích, technických stavech, atd. Retranslace se provádí rychlostí 300 tagù FLA /sek. Tento retranslační proces se periodicky opakuje každé 3 sekundy. Vyhodnocovací centrální jednotka FLU pak všechny tyto informace předává nadřazenému EZS systému nebo přímo řídí polohování PTZ kamer. Max. doba zpoždění, od incidentu narušení perimetru do okamžiku, kdy centrální jednotka FLU vyhlásí alarm, je tedy dána součtem "periody retranslace"+"doby retranslace k nejbližší jednotce FLM". [9].



Obr. 39 Princip detekce klimatických vlivů

3.1.4.5.1. Princip detekce pachatele a klimatických rušivých vlivu a umělá inteligence.

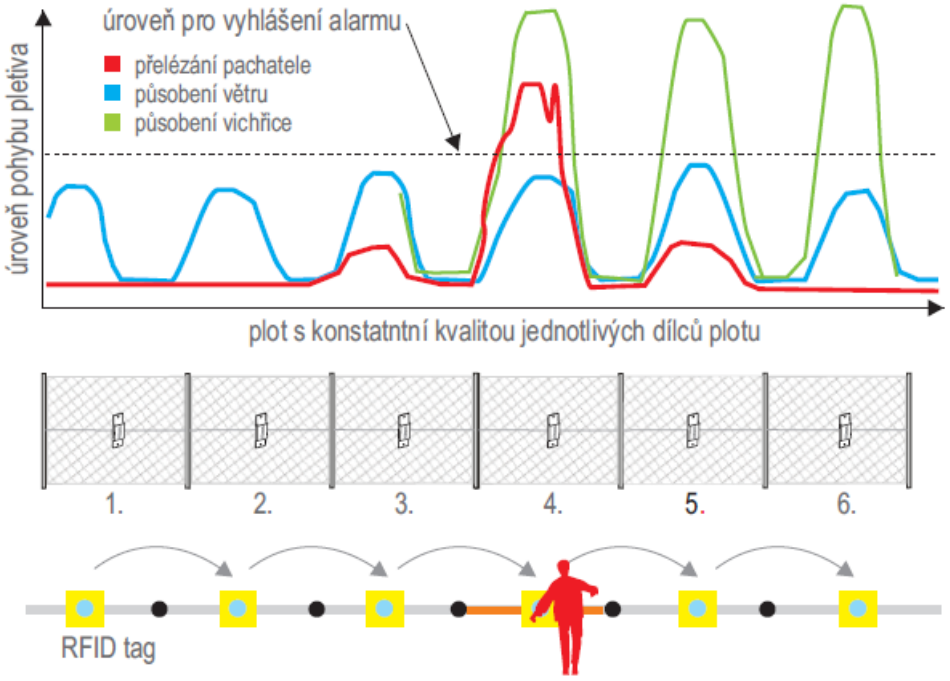
Detektory snímají časové a dynamické změny v poloze pletiva, které jsou typické pro přelézání plotu narušitelem. Vzhledem k tomu, že se signály ze všech RFID detektorů vyhodnocují paralelně, umí perimetrický systém eliminovat falešné poplachy vzniklé působením větru, dešti, krupobitím nebo blízké dopravy na pletivo, protože takto vyvolané změny působí v jednom okamžiku na více než jeden RFID detektor současně. RFID detektory se díky sofistikované analýze pohybu automaticky kalibrují a přizpůsobují měnící se mechanické kvalitě jednotlivých dílců plotu (např. způsobené uvolněním závěsů plotu). [9].

3.1.4.5.2. Princip odolnosti vichru, vichřice atd.

Protože systém Perimetr Locator umožňuje detekovat silný vítr a jiné klimatické vlivy působící na plot a to i v případě, že naměřené signály při působení vichřice budou mnohem větší než nastavená úroveň pro vyhlášení alarmu narušitelem, falešné alarmy nevyhlašuje. Disponuje tedy komfortním širokým pásmem pro nastavení vhodné úrovně alarmu a technikům tedy nevnucuje nutnost kompromisů při nastavování citlivosti.

Systém navíc díky své umělé inteligenci provádí automatickou korekci signálů z detektorů na vadných dílcích plotu nebo v případě, kdy je tag FLA paralyzován kusem ledu na plotě.

Instalace detektorů FLA-04 se provádějí tak, aby byly orientovány logem směrem nahoru a dovnitř perimetru, viz obr. 40. Instalují se svisle na drátěné pletivo plotu sešroubováním s nerezovým protikusem a s krycím plechem v ose středového napínacího drátu. [9].



Obr. 40 Plot s konstantní kvalitou jednotlivých dílců plotu

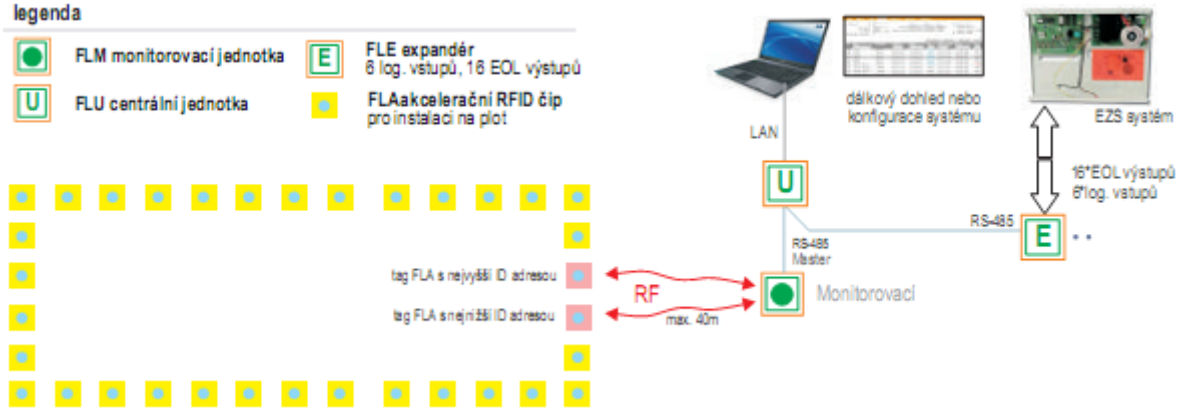
Obr. 41 RFID detektor FLA

3.1.4.5.3. Instalace perimetru

Pro samotnou instalaci použijeme systém uzavřeného perimetru, kdy vždy do jednoho pole plotu uprostřed upevníme RFID detektor FLA-02 podle návodu, a to na vnitřní stranu plotu z pohledu chráněného objektu přišroubovaný proti nerezové podložce. Detektory FLA umí detekovat jakoukoliv snahu o odcizení detektoru nebo o sabotáž demontáží, a to i v denním režimu. Jsou bezúdržbové s životností 10-15 let a odolávají povětrnostním vlivům díky krytí IP68. Celá elektronika je zalita

speciální hmotou do jednolitého celku velmi pevné konstrukce. Detektor FLA s nejnižší a nejvyšší IP adresou bude připevněn na dílcích plotu nejblíže u budovy II, na které bude upevněna monitorovací jednotka FLM-02. Tato jednotka bude napojena sběrnicí RS-485 na centrální jednotku FLU-02, kde probíhá hlavní diagnostika, konfigurace, logování a dohled perimetrického systému. Centrální jednotka FLU má vlastní IP adresu a umožňuje připojení do LAN sítí pro potřebu dálkového dohledu.

Disponuje pamětí pro automatické ukládání historie všech událostí, jako jsou provozní stavy, poplachy, sabotáže, technické poruchy atd. Jednotka FLU má optický tamper a sofistikovanou detekci odejmutí jednotky z montážní podložky a navrtání víka narušitelem, umí detekovat ztrátu komunikace s expandérem FLE nebo s monitorovacími jednotkami FLM na sběrnici RS 485 a sepnout sabotážní výstup, má 8 programovatelných vstupů / výstupů s otevřeným kolektorem a 2 relé, které lze využít pro řízení vysílače na PCO, ATH komunikátoru, sirén, světel atd. Centrální jednotka FLU komunikuje po sběrnici RS485 s expandérem FLE, prostřednictvím kterého se systém propojuje s EZS ústřednou.



Obr. 42 Zapojení modulu FLU

Kabeláž sběrnice bude natažena kabelem FTP, ve vnějším prostoru FTP outdor, chráněné v trubce. Napájení napojeno kabelem CYKY – J 3x1,5 ze samostatně jištěného vývodu 230V/10A. Centrální jednotka je zálohována dobíjeným akumulátorem 12V/17Ah. Systém by měl splňovat požadavky ČSN EN 50131 na dobu zálohování 12h pro stupeň zabezpečení 2. [9].

3.1.5. Bezpečnost a ochrana zdraví při práci

Při souběhu slaboproudých rozvodů se silovým vedením nn z pohledu vzájemného ovlivňování se je nutné respektovat příslušná ustanovení ČSN 34 2305, z pohledu bezpečnosti pak ČSN 34 2300 a ČSN 34 1050.

- Montážní práce elektro smí provádět organizace mající oprávnění k montážním činnostem v příslušné kategorii elektrotechnické působnosti.
- Pracovníci provádějící montáž musí mít platné oprávnění, potvrzující příslušnou elektrotechnickou kvalifikaci, včetně zdravotní způsobilosti.

- Pracoviště, tj. prostory montáže, musí být zbaveno hrubých mechanických překážek (stavební materiál, rozměrné předměty apod.).
- Elektrické nářadí používané při montáži musí být podrobeno předepsaným revizním zkouškám, zkoušky musí být opakovány v předepsaných intervalech.
- Pomocné prostředky, a. j. žebříky, plošiny či lešení musí být pouze tovární výroby, řádně evidované a podrobené pravidelným revizím.
- Při práci v prostorách s nebezpečím pádu předmětů z výšky musí být používáno ochranných přileb.
- Při práci ve výškách musí být dbáno na řádné zabezpečení osob např. bezpečnostními pásy.
- Na pracovišti musí být vždy k dispozici řádně vybavená lékárna první pomoci, doplněná aktuálním traumatologickým plánem.
- Při manipulaci na elektrických zařízeních musí být dodržována pravidla ochrany před nebezpečným dotykovým napětím dle souboru základních norem řady ČSN 33 2000 DX.
- Během realizace musí být dodržovány normy ČSN, ON, včetně harmonizovaných norem ČSN/DIN, ČSN/IEC, ČSN/LPCB, technické podmínky jednotlivých výrobků a související předpisy, jako je vyhláška 4. 324/1990 Českého úřadu bezpečnosti práce a Českého báňského úřadu. Při montáži musí být dbáno na veškerá nařízení ochrany zdraví a bezpečnosti při práci, včetně dodržování pravidel požární bezpečnosti, popř. zvláštních hygienických předpisů.

Poznámka: Uvedený přehled opatření bezpečnosti a ochrany zdraví při práci doplňuje projektovou dokumentaci ve smyslu platných předpisů, ale nenahrazuje vlastní bezpečnostní předpisy montážní a dodavatelské firmy k problematice BOZ a požární ochrany.

3.1.6. Vnější vlivy

Působení vnějších vlivů bylo posuzováno dle ČSN 33 2000 – 3 a je součástí projektové dokumentace silnoproudu.

3.1.7. Elektromagnetická kompatibilita (EMC)

Dle zákona o technických požadavcích na výrobky č. 22/97 Sb. nařízení vlády č. 169/97 Sb. musí být přístroje včetně vybavení a instalací provedeny a instalovány tak, aby elektromagnetické rušení, které způsobují, nepřesáhlo povolenou úroveň a naopak musí mít odpovídající odolnost vůči vystavenému elektromagnetickému rušení, která jim umožňuje provoz v souladu se zamýšleným účelem.

3.1.8. Závěr technické zprávy

Veškeré práce budou provedeny v souladu s příslušnými normami ČSN a technickými předpisy. Ochrana před nebezpečným dotykovým napětím:
Dle ČSN 332000-4-41 Malým napětím SELV

Ochrana před škodlivými vlivy na životní prostředí
Při provozování i eventuální poruše zařízení nejsou žádné škodlivé vlivy na životní prostředí. Bezpečnost práce je zajištěna krytím, isolací a ochranou před nebezpečným dotykovým napětím.

3.2. Rozpočet a kalkulace nákladů

V této části jsem zpracoval předběžný rozpočet, který je rozdělen podle návrhu systémů a nakonec jsem porovnal rozpočet se stávajícími náklady na provoz a ochranu majetku bezpečnostní agenturou.

Rekapitulace nákladů bez DPH	
Kontrola vjezdu (brána, závora)	97 193 Kč
Kontrola přístupu	164 112 Kč
Perimetr Locator	307 985 Kč
Náklady celkem	**569 290 Kč**

Tab. 4 Rekapitulace nákladů bezpečnostních systémů

Kalkulace nákladů - brána

Brána				
Označení	**Popis komponent**	**Cena MJ**	**MJ**	**Celkem**
TOONAKIT	řídící jednotky MC824H	4 237,00	1	4 237,00
	elektromechanických pohonů Toona4024 (TO4024)	4 612,00	2	9 224,00
	pár bezpečnostních fotobuněk MOFB	975,00	1	975,00
	MOCF - sloupek pro fotočlánek MOF	460,00	2	920,00
	PCM - základová deska s kotevními háky do betonu	180,00	2	360,00
	výstražný maják LUCY	403,00	1	403,00
	ABFKIT - anténa	246,00	1	246,00
	RTU5015 - profesionální gsm ovladač	5 687,00	1	5 687,00
	FLO2R - dvoukanálový dálkový ovladač Nice	475,00	2	950,00
	SMXI - zásuvný čtyřkanálový deskový přijímač	561,00	1	561,00
	instalační materiál (kabel, krabice, trubky, apod.)	3 000,00	1	3 000,00
Závora				
Signo 6 kit	Signo6 Kit - sada rychlé automatické závory s ramenem 6.25 m	31 224,00	1	31 224,00
	pár bezpečnostních fotobuněk MOFB	975,00	2	1 950,00
	MOCF - sloupek pro fotočlánek MOF	460,00	6	2 760,00
	PCM - základová deska s kotevními háky do betonu	180,00	6	1 080,00
	instalační materiál (kabel, krabice, trubky, apod.)	3 000,00	1	3 000,00
MREM 63-TF	Čtecí modul 125 kHz (EM/HID), 2x vstup, 2x výstup, RS485, wiegand, IP 54, 2 prog. karty, černý	5 280,00	2	10 560,00

Rekapitulace nákladů bez DPH		
Materiál celkem		77 137,00
Montáže	20%	15 427,40
Stavební připravenost	6%	4 628,22
Náklady celkem		**97 193 Kč**

Tab. 5 Kalkulace - brána

Kalkulace nákladů - přístup

Označení	Popis komponent	Cena MJ	MJ	Celkem
2 podlaží				
MREM 63-TF	Čtecí modul 125 kHz (EM/HID), 2x vstup, 2x výstup, RS485, wiegand, IP 54, 2 prog. karty, černý	5 280,00	3	15 840,00
APSLAN	Převodník RS485/Ethernet pro systémy APS mini Plus a APS mini Plus	2 368,00	1	2 368,00
REP 485	Opakovač linky pro systémy APS, galvanické oddělení	1 800,00	0	0,00
AKU 12V/17Ah	Akumulátor 12V/17 Ah	646,00	1	646,00
KPN-18-30LAW	Napájecí zdroj lineární 13,8V/3A, ocelová skříň, prostor na AKU 12V/18Ah	2 338,00	1	2 338,00
	elektrický zámek BEFO 211211	1 224,00	3	3 672,00
	instalační materiál (kabel, krabice, lišty, apod.)	2 000,00	1	2 000,00
1 podlaží				
MREM 63-TF	Čtecí modul 125 kHz (EM/HID), 2x vstup, 2x výstup, RS485, wiegand, IP 54, 2 prog. karty, černý	5 280,00	10	52 800,00
APSLAN	Převodník RS485/Ethernet pro systémy APS mini Plus a APS mini Plus	2 368,00	1	2 368,00
REP 485	Opakovač linky pro systémy APS, galvanické oddělení	1 800,00	0	0,00
AKU 12V/17Ah	Akumulátor 12V/17 Ah	646,00	1	646,00
KPN-18-90LAW	Napájecí zdroj lineární 13,8V/7+2A, ocelová skříň, prostor na AKU 12V/18Ah	3 980,00	1	3 980,00
Card TF R/O	Karta TF s popisem	30,00	50	1 500,00
	elektrický zámek BEFO 211211	1 224,00	8	9 792,00
	elektromechanický zámek BERA-D se signalizací a kováním	7 250,00	2	14 500,00
	instalační materiál (kabel, krabice, lišty, apod.)	5 000,00	1	5 000,00
CCTV				
AVN222	dome IP kameru s kompresí H.264 a variobjektivem	4 440,00	3	13 320,00
AVN263ZP_12V	venkovní barevná IP-kamera s IR přisvětlením (40 metrů)	5 990,00	1	5 990,00
	instalační materiál (kabel, krabice, lišty, apod.)	3 000,00	1	3 000,00

Rekapitulace nákladů bez DPH		
Materiál celkem		136 760,00
Montáže	20%	27 352,00
Stavební připravenost	0%	0,00
Náklady celkem		**164 112 Kč**

Tab. 6 Kalkulace - přístup

Kalkulace nákladů - perimetr

Perimetr Locator

Označení	Popis komponent	Cena MJ	MJ	Celkem
FLA-02	detektor RFID	1 995,00	137	273 315,00
FLU	centrální jednotka	7 900,00	1	7 900,00
FLE	expandér k FLE	5 900,00	1	5 900,00
FLM	monitorovací jednotka	8 900,00	1	8 900,00
				0,00
				0,00
				0,00
				0,00
				0,00
				0,00
	instalační materiál (kabel, krabice, trubky, apod.)	3 000,00	1	3 000,00

Rekapitulace nákladů bez DPH		
Materiál celkem		299 015,00
Montáže	3%	8 970,45
Stavební připravenost	0%	0,00
Náklady celkem		**307 985 Kč**

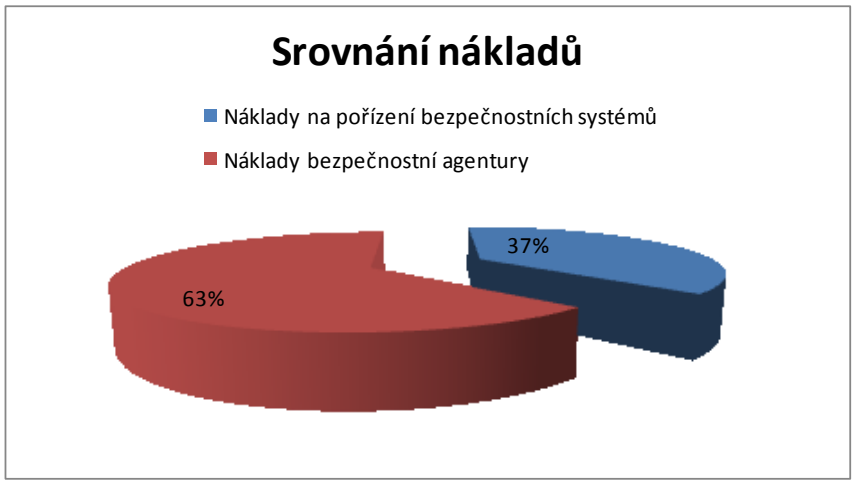
Tab. 7 Kalkulace - perimetr

3.3. Kalkulace a srovnání se současným stavem

Stávající ochrana objektu je nyní zabezpečována bezpečnostní agenturou ve formě stálé služby, jedním strážným po nepřetržitou dobu 24 hodin denně. V pracovní dny má strážný v popisu práce kontrolu a identifikaci vozidel, vjíždějících do areálu a zajištění správní budovy před vstupem mimo úřední hodiny na vrátnici. Po pracovní době, většinou od 7:00 hod do maximálně 18:00 hod a po opuštění všech zaměstnanců a firem, uzavře areál vstupní branou a přebírá jeho ostrahu. V nočních hodinách a všedních dnech je areál v kompetenci jediného strážného. V minulosti nastaly i případy narušení objektu včetně spáchání trestného činu vloupání a krádeže. Toto zabezpečení se v této chvíli stává jako neekonomické a nesplňující svou podstatu.

Rekapitulace nákladů bez DPH		
Náklady bezpečnostní agentury	1 hodina	110 Kč
	1 den	2 640 Kč
		0 Kč
Náklady celkem za 1 rok		**963 600 Kč**

Tab. 8 Rekapitulace nákladů ochrany objektu za 1 rok



Graf 1 Grafické srovnání nákladů

Tato studie a návrh by měla plně zabezpečit areál před nezvanými návštěvníky s daleko větším komfortem, účelovostí a bezpečnosti. Při narušení zabezpečení perimetrie a vyvolání poplachu systém, napojený na EZS, odešle varovné SMS zprávy na nastavená telefonní čísla a vyvolá poplach na pult centralizované ochrany PCO. Určené osoby mají možnost se okamžitě podívat pomocí sítě Internetu na aktuální stav v objektu a vyhodnotit tak situaci. Na srovnávacím grafu vidíme jasnou a brzkou návratnost investic do těchto na sobě závislých a spolupracujících systémů, které se můžou dále rozšiřovat a modifikovat bez větších zásahů do instalací. Například o již zmíněné PTZ kamery pro

zajištění ještě větší bezpečnosti ve vnějších částech areálu nebo integrace dalších systémů automatizace v kancelářské budově napojených na kontrolu vstupu. Jako příklad můžu uvést řízení osvětlení na chodbách a v kancelářích v závislosti na adresném přihlášení do systému, jakož i ovládání ventilace a topení, ovládání žaluzií, apod.

4. Závěr

Závěrem bych chtěl podotknout, že pokud chceme, aby naše budovy splňovaly budoucí potřeby, musí být požadavky kladené na současné systémy budov velmi náročné. Vedle optimální funkčnosti a bezpečnosti musí být kladen důraz také na uživatelsky příjemné ovládání na všech úrovních systému. A zde se uplatní výhody moderních automatizačních systémů budov jako snadno pochopitelné informace, rychlý přístup k jednotlivým událostem a jednoduché ovládání.

V mojí diplomové práci jsem se zaměřil pouze na jednu část systémů, bezpečnost, ale vývoj, požadavky a nároky jdou neustále dopředu, kdy současnou hlavní prioritou je tzv. „management energetického hospodářství“. Není – li provoz systémů optimalizovaný z hlediska spotřeby energií, může být výsledkem značné zvýšení provozních nákladů. Určité úspory lze dosáhnout vhodnou organizací práce a časovým rozvrhem aktivity pracovišť a doby provozu energeticky náročných spotřebičů, ovšem k efektivnímu řešení této problematiky je nezbytná technická podpora integrovaného řídicího systému budov.

Literatura:

[1]. Hermann Merz a kol. *Automatizované systémy budov.* 1. vydání Praha: Grada Publishing. 2009. 261 s. ISBN 978-80-247-2367-9 (brož.)

[2]. URL: < http://cs.wikipedia.org/wiki/>

[3]. URL: < http://vytapeni.tzb-info.cz/mereni-a-regulace/6879-systemy-pouzivane-v-inteligentnich-budovach-prehled-komunikacnich-protokolu> [cit. 2010-10-25]

[4]. URL: < http://vytapeni.tzb-info.cz/mereni-a-regulace/7011-systemy-a-komponenty-pouzivane-pro-automatizaci-budov-integrace-systemu > [cit. 2010-12-13]

[5]. URL: < http://cs.wikipedia.org/wiki/RFID > [cit. 2011-03-01]

[6]. URL: < http://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm> [cit. 2004-03]

[7]. Pištěk Karel. *Multitechnologicke pristupove karty.pdf*. Security World. červen 2009. 2/2009. [cit. 2009-06]. Dostupné z <http://www.sovte.cz/media.php>

[8]. *Zabezpecovaci_system_i_net_seven.pdf.* Praha: Schneider Electric CZ, s.r.o. [cit. 2008-08]

[9]. *Instal- Manua_ Perimetr_ Locator_7.2.2011.pdf. 7Marsyas Development a.s.* [cit. 2011-02-07]

Přílohy: